DOCUMENT RESUME

ED 380 136 IR 055 440

TITLE	Information Superhighway: An Overview of Technology Challenges. Report to the Congress.
INSTITUTION	General Accounting Office, Washington, D.C.
REPORT NO	GAO/AIMD-95-23
PUB DATE	Jan 95
NOTE	85p.
PUB TYPE	Legal/Legislative/Regulatory Materials (090)
EDRS PRICE	MF01/PC04 Plus Postage.
DESCRIPTORS	Communications; *Computer Networks; *Computer Security; Confidentiality; Cooperation; Information Networks; Planning; Privacy; *Reliability; Standards; *Technological Advancement; User Needs (Information); Users (Information)
IDENTIFIERS	Information Superhighway; *Interoperability; *National Information Infrastructure

ABSTRACT

This report focuses on the pivotal technical issues associated with the National Information Infrastructure program, security and privacy, interoperability, and reliability, and presents the General Accounting Office's findings on these challenges. It is reported that while the structures and services to be offered by the information superhighway have not yet been determined, several critical technological challenges are emerging. First, if it is to provide critical communications services to manufacturing, health care, and other business sectors, the superhighway must ensure data security and protect users' privacy. Second, the superhighway should provide a seamless web of features and services to users, with thousands of systems and components interacting, or interoperating, in a way that is transparent to users. Achieving interoperability will require manufacturers to cooperate with standards-setting bodies to establish common interfaces and protocols. Third, to prevent network failures, the superhighway must be reliable, end-to-end, from users to service providers. Five appendices provide information on the technical issues addressed by the information infrastructure task force; descriptions of existing network technologies and advanced technologies; the portability of telephone numbers; and major contributors to this report. Sixteen figures illustrate the text, and a 15-page glossary defines the technological terms. (Author/MAS)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

United States General Accounting Office

GAO

Report to the Congress

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☐ This document has been reproduced as received from the person or organization originating it

☐ Minor changes have been made to improve reproduction quality

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy

January 1995

INFORMATION SUPERHIGHWAY

An Overview of Technology Challenges

ED 380 136

BEST COPY AVAILABLE

IR055440

Notice: This is a reprint of a GAO report.

GAO

United States
General Accounting Office
Washington, D.C. 20548

Comptroller General
of the United States

B-259205

January 23, 1995

To the President of the Senate and the
Speaker of the House of Representatives

In light of the strategic importance of the information superhighway, we summarized the socioeconomic, regulatory, and technical issues associated with its development in a September 1994 report. The enclosed report focuses in more detail on the major technical issues facing the industry and federal regulators in planning and implementing the superhighway.

We are sending copies of this report to all Members of Congress; the Secretary of Defense; the Secretary of Commerce; and the Chairman, Federal Communications Commission. Copies will also be made available to others on request.

This report was prepared under the direction of Joel C. Willemssen, Director, Information Resources Management/Resources, Community, and Economic Development Issues, who can be reached at (202) 512-6253. Other major contributors to this report are listed in appendix V.

Charles A. Bowsher
Comptroller General
of the United States

Executive Summary

Purpose

To take advantage of emerging technologies to create, manage, and use information that could be of strategic importance to the United States, the administration has launched an ambitious initiative—known as the National Information Infrastructure program—to guide industry's development of the national information superhighway. The Congress, while sharing the administration's vision, has been examining what impact the high stakes race among the major industry players to carve out portions of the superhighway will have on competition and service choices.

Because of the importance of the information superhighway, GAO initiated work to identify the socioeconomic, regulatory, and technical issues associated with this initiative in detail. GAO summarized these issues in a prior report.[1] This current report focuses in more depth on the pivotal technical issues—security and privacy, interoperability, and reliability. Failure by the private and public sectors to address these challenges could adversely affect the future of the emerging information superhighway.

Background

The administration envisions the superhighway as a seamless web of communications networks, computers, databases, and consumer electronics—built, owned, and operated principally by the private sector—that will put vast amounts of information at users' fingertips. It believes that the superhighway, if freed from the constraints imposed by rigid regulatory regimes, can fundamentally change the way we work, learn, get health care and public services, shop, communicate, and entertain ourselves.

While initial versions of some of these advanced capabilities and services are already provided by the existing infrastructure, albeit at relatively high cost and low transmission speeds, much remains to be done to achieve the superhighway's potential. For example, although some of the services envisioned for the information superhighway are being provided by the Internet, various on-line information services, and thousands of electronic bulletin boards, these services are not ubiquitous, secure, or consistently user friendly. Building the superhighway will require deploying and integrating advanced communications technologies with the existing communications networks, and investing tens of billions of dollars to build the "on ramps" to connect residential, institutional, and business users.

[1]Information Superhighway: Issues Affecting Development (GAO/RCED-94-285, Sept. 30, 1994).

The administration has formed a multiagency group—the Information Infrastructure Task Force—to articulate a vision for the information superhighway and to guide its development. The task force is examining a wide range of technical issues relevant to the development and growth of the superhighway.

Results in Brief

While the structure and services to be offered by the information superhighway have not yet been determined, several critical technical challenges are emerging. First, if it is to provide critical communications services to manufacturing, health care, and other business sectors, the superhighway must ensure data security and protect users' privacy. Because existing public networks are largely unsecured and are vulnerable to damage from intruders, achieving security and privacy will require careful and thoughtful design.

Second, the superhighway should provide a "seamless" web of features and services to users, with thousands of systems and components interacting, or interoperating, in a way that is transparent to users. Achieving interoperability will require manufacturers to cooperate with standards-setting bodies to establish common interfaces and protocols.

Third, to prevent network failures, the superhighway must be reliable, end-to-end, from users to service providers. Recent outages on the existing networks that will form the foundation for the superhighway have raised concerns about achieving this goal.

Principal Findings

Ensuring Security and Privacy Will Pose a Major Challenge

A large volume of the information that will traverse the superhighway will be proprietary or privacy sensitive and therefore will need to be protected. Unauthorized disclosure, theft, modification, or malicious destruction of such information could bankrupt a business, interrupt vital public service, or destroy lives. As it evolves, the infrastructure will likely become a tempting target for intruders with the technical expertise and resources to cause great harm. These intruders could include hackers, foreign governments conducting political and military intelligence operations, domestic and foreign enterprises engaged in industrial espionage, or terrorist groups seeking to disrupt our society or cripple our economy.

Significant effort will be needed to define, develop, test, and implement measures to overcome the security challenge posed by the development of the superhighway. These measures include identifying the superhighway's security and privacy requirements and developing tools and techniques to satisfy the requirements.

The federal government, because of its extensive experience and expertise in developing secure networks, could play a leading role in ensuring the superhighway's security. However, critics of federal involvement argue that current federal initiatives represent a danger to civil liberties, and that individuals should be free to choose the technical means for achieving information security. As a result, the challenge will be establishing a reasonable level of consensus among the major players—the government, the computer and communications industry, the business community, and civil liberty groups—on how to ensure information security and privacy.

Achieving Interoperability Is a Critical Goal

An essential goal of the superhighway will be achieving interoperability among the thousands of networks and components. Such interoperability is critical for ensuring the delivery of seamless features and services to users.

Achieving this goal will be difficult because the components and services of the superhighway will be designed, provided, and maintained by thousands of suppliers. Further, ensuring interoperability will also require the development and use of standards for voice, video, data, and multimedia services. However, many of the standards needed to ensure the superhighway's interoperability do not currently exist, while in other cases, systems, including digital cellular system and some high-speed optical transmission systems, are being deployed based on ill-defined, immature, or competing standards. The federal and private sectors are beginning to deal with certain aspects of network interoperability, such as the development of industry-wide standards and the establishment of interoperability test beds.

Network Reliability Is Emerging as a Key Challenge

The superhighway will rely on complex hardware and software components to link thousands of networks serving hundreds of millions of users worldwide. While these components are beginning to provide a host of new services, they are also becoming one of the largest causes of network failures. As fewer and fewer components handle more and more connections, a failure of one component could cause the loss of service for

several million customers. In addition, the introduction of new technologies and growth in the number of networks will likely increase vulnerability. The government and industry have recently taken steps, including the establishment of the Network Reliability Council and the Networks Operations Forum, to address these issues.

Recommendations

Because this report is intended to serve as an overview of key technical issues, it makes no recommendations.

Agency Comments

GAO provided and discussed a draft of this report with officials from the Federal Communications Commission, the National Telecommunications and Information Administration, the Information Infrastructure Task Force, the National Institute of Standards and Technology, the Department of Defense, the Advanced Research Projects Agency, and the National Security Agency. These officials generally agreed with the contents of this report. GAO incorporated their comments where appropriate.

Contents

Executive Summary		2
Chapter 1 Introduction		10
	The Grand Vision of the Information Superhighway	11
	Objective, Scope, and Methodology	16
Chapter 2 Ensuring Security and Privacy Will Pose a Major Challenge		18
	Networks and Computer Systems Are Increasingly Vulnerable to Attacks	19
	Security Measures Are Critical to Minimizing Risk	20
	Federal Role in Security and Privacy Is Subject to Debate	23
Chapter 3 Achieving Interoperability Is a Critical Goal		31
	Interoperability Will Be Difficult to Achieve	31
	The Federal and Private Sectors Have Initiated Efforts to Address Interoperability	33
Chapter 4 Network Reliability Is Emerging as a Key Challenge		35
	Reliability of the Superhighway Will Be Essential	35
	The Government and Industry Are Taking Steps to Address Reliability	39
Chapter 5 Conclusions		41
Appendixes		
	Appendix I: Information Infrastructure Task Force Is Addressing Selected Technical Issues	42
	Appendix II: Description of Existing Network Technologies	45
	Appendix III: Description of Advanced Technologies	53
	Appendix IV: Ensuring the Portability of Telephone Numbers Poses a Challenge	62
	Appendix V: Major Contributors to This Report	65
Glossary		66

Related GAO Products 84

Figures

Figure 1.1: Functional Layers of the Information Superhighway 12
Figure 1.2: Telephone, Cable, and Wireless Networks 15
Figure 2.1: Secret and Public Key Encryption Systems 22
Figure 2.2: Tessera Crypto Card 23
Figure 2.3: The Capstone and the Clipper Chips 26
Figure 2.4: Message Encrypted With the Pretty Good Privacy Encryption System 30
Figure 4.1: Fiber Optic Cable "Dig-up" Accident 38
Figure II.1: A Typical Local Telephone Network 47
Figure II.2: A Typical Cable System Architecture 48
Figure II.3: A Typical Cellular System Architecture 50
Figure II.4: Broadcast and VSAT Satellites 52
Figure III.1: ISDN Architecture 54
Figure III.2: AIN Architecture 56
Figure III.3: B-ISDN Architecture 57
Figure III.4: Low Earth Orbit Satellite System 59
Figure III.5: Broadband in the Local Loop 61

BEST COPY AVAILABLE

Abbreviations

AIN	advanced intelligent network
ARPA	Advanced Research Projects Agency
ATM	asynchronous transfer mode
B-ISDN	Broadband Integrated Services Digital Network
DOD	Department of Defense
FCC	Federal Communications Commission
GEO	geosynchronous Earth orbit
HPCC	High Performance Computing and Communications
Hz	Hertz
IDEA	international data encryption algorithm
IITF	Information Infrastructure Task Force
ISDN	integrated services digital network
Kbps	thousand bits per second
LAN	local area network
LEO	low Earth orbit
Mbps	million bits per second
NANP	North American Numbering Plan
NII	national information infrastructure
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSI	Office of Special Investigations
PCN	personal communications network
PCS	personal communication system
SAC	service access code
SONET	synchronous optical network
SS7	Signaling System 7
VF	voice frequency
VSAT	very small aperture terminal

Introduction

A global technological upheaval, fueled by rapid advances in information processing, storage, switching, and transmission technologies, is beginning to blur the lines between computing, telephony, television, and publishing. This convergence is creating a new breed of information service industry, and permitting the development of the much discussed National Information Infrastructure (NII), commonly known as the information superhighway. The administration envisions the superhighway as a seamless web of communications networks, computers, databases, and consumer electronics—built, owned, and operated principally by the private sector—that will put vast amounts of information at users' fingertips. It believes that the superhighway, if freed from the constraints imposed by rigid regulatory regimes, will fundamentally change the way we work, learn, shop, communicate, entertain ourselves, and get health care and public services.

Despite the dramatic advances in technology and the changes sweeping the communications industry, the superhighway's development is expected to be slow and arduous. As such, its development should not be viewed as a cliff that is suddenly confronted, but rather an increasingly steep slope that society has been climbing since the early communications networks were established.[1] A national and global information infrastructure, which will serve as the foundation for the superhighway, already exists. Telephones, televisions, radios, computers, and fax machines—interconnected through a complex web of fiber optics, wires, cables, satellites, and other communications technologies—are used every day to receive, store, process, display, and transmit data, text, voice, sound, and images in homes and businesses throughout the world. However, the information superhighway is expected to offer much more than separate telephone, data, or video services; it is expected to integrate these services into an advanced high-speed, interactive, broadband, digital communications system.[2]

Some of the advanced capabilities and services envisioned for the superhighway are beginning to be provided—albeit at a relatively high cost and at low transmission speeds—by the existing information

[1]What it Takes to Make It Happen: Key Issues for Applications of the National Information Infrastructure, Committee on Applications and Technology, Information Infrastructure Task Force, January 25, 1994.

[2]In digital networks, analog messages (such as voice) are converted to digital signals (ones and zeroes). Once in digital form, voice, video, graphics, and text can be combined and efficiently stored, compressed, and transmitted. The capacity of a digital network may be described in terms of the number of bits that the network can transmit every second. In general, narrowband networks transmit at rates below 1.5 million bits per second (1.5 Mbps), broadband networks transmit at rates above 1.5 Mbps.

infrastructure. For example, the Internet—a global metanetwork, or "network of networks," linking over 59,000 networks, 2.2 million computer systems, and over 15 million users in 92 countries—provides many of the services envisioned for the information superhighway.[3] Similarly, a growing number of on-line services, such as CompuServe, America Online, and Prodigy, provide their subscribers with a rich array of information services. Finally, hundreds of communities across America are served by electronic bulletin boards dispensing information to hundreds of thousands of users.

The administration, believing that the technologies to create, manipulate, manage, and use information are of strategic importance to the United States, has formed a multiagency group—the Information Infrastructure Task Force (IITF)—to articulate a vision for the information superhighway and to guide its development. The task force, chaired by the Secretary of Commerce, is responsible for addressing a wide range of regulatory and technical issues related to the information superhighway and for the coordination of existing federal efforts in the communications area. The task force is examining, through its committees and working groups, a wide range of technical issues relevant to the development and growth of the information superhighway. A more detailed description of the IITF structure and its activities is presented in appendix I.

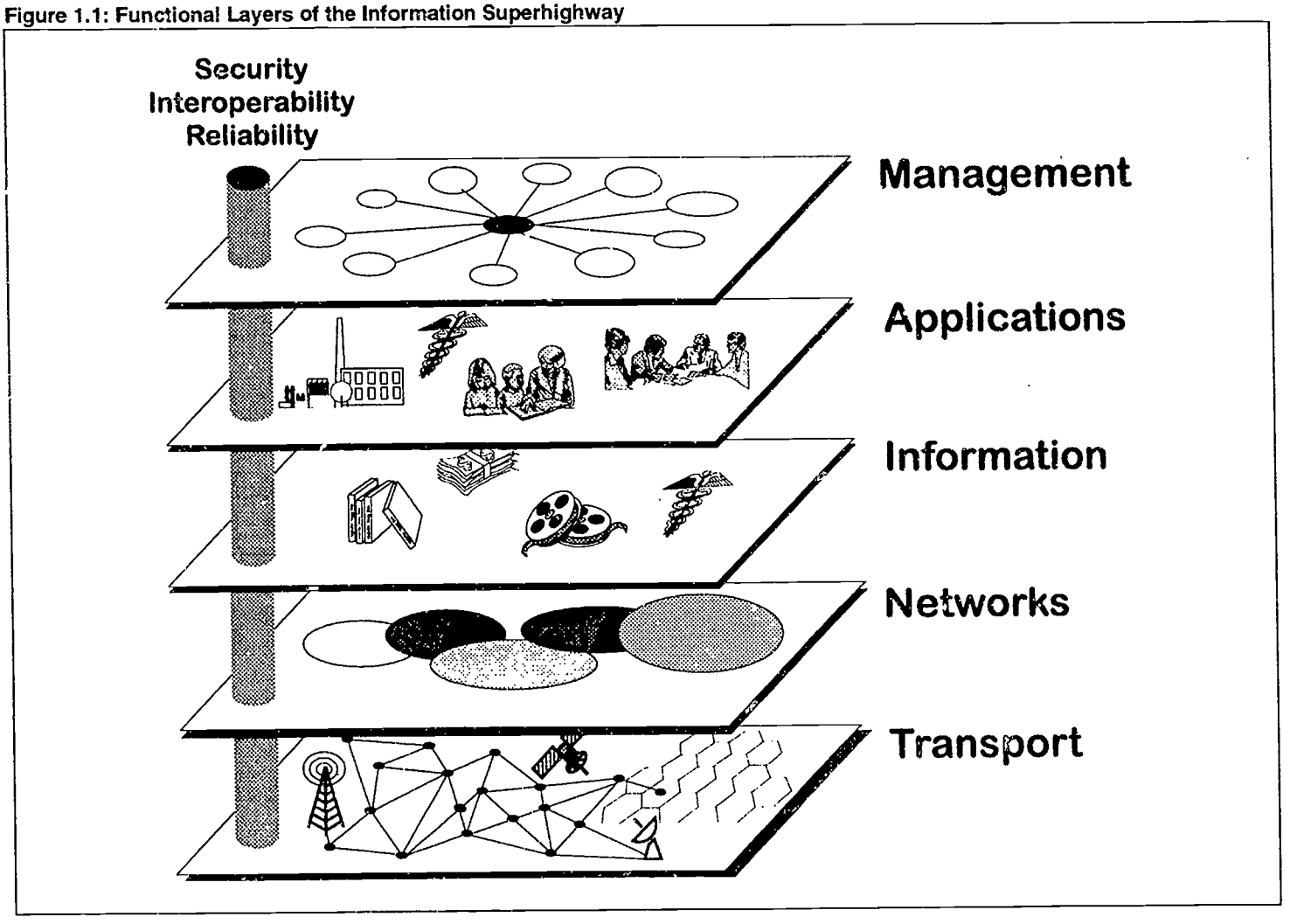
The Grand Vision of the Information Superhighway

While industry is beginning to build the information superhighway, little is known about how the superhighway will be structured and what services it will provide. Nevertheless, a common vision of its capabilities is beginning to form among policymakers and public interest groups. First, there is an emerging agreement that the superhighway should be structured as a metanetwork that will seamlessly link thousands of broadband digital networks. Second, it should allow a two-way flow of information, with users being able to both receive and transmit large volumes of digital information. Third, it should be open, ensuring equal access for service and network providers. Finally, it should ensure the security and privacy of databases and users' communications, and provide a high degree of interoperability and reliability.

[3]Internet users with access to a transmission speed of 56 thousand bits per second (56 Kbps) can receive digital radio or transmit and receive digital files containing embedded text, voice, video, and images. However, at current commercial rates, the average fee for attachment to the Internet at 56 Kbps is about $15,000 per year. Users not requiring sophisticated multimedia services may access Internet for about $25 per month.

Achieving the grand vision will depend largely on how successfully industry integrates advanced technologies and capabilities into the various layers of the information superhighway. To better understand the integration of advanced telecommunication technologies into the existing communication infrastructure, we developed a conceptual model of the information superhighway, as shown in figure 1.1.

Figure 1.1: Functional Layers of the Information Superhighway



The model presents the following five critical layers—management, applications, information, networks, and transport—linked with pervasive security, interoperability, and reliability requirements:

- the transport layer consists of optical fibers, coaxial cable, copper wire, switches, routers, satellites, and transmitters
- the networks layer consists of thousands of logical networks superimposed on the transport layer
- the information layer includes databases and electronic libraries containing text, images, and video
- the applications layer contains software and consumer electronics needed to access the superhighway's information and services
- the management layer consists of operations and administrative centers, emergency response teams, and security services.

Today's Networks Provide the Foundation for the Superhighway

With a few exceptions, such as the recently proposed global satellite networks, most experts anticipate that the superhighway will be built on the foundation of the existing communications infrastructure. Over the years, this infrastructure has evolved into three separate, and frequently incompatible, communications networks.[4] These are

- the wire-based voice and data telephone networks,
- the cable-based video networks, and
- the wireless voice, data, and video networks.

The wire-based voice and data telephone networks are part of the global telephone network.[5] The voice networks provide ubiquitous, highly interoperable, high-speed, and flexible telephone service to millions of users. The data networks provide high-speed digital data communications services. The cable-based video networks rely on various approaches to broadcast a one-way broadband video signal to individual subscribers. Finally, the wireless networks use a wide range of analog and digital radio technologies to deliver voice, data, and video services.

The principal shortcoming of the existing communications infrastructure is its inability to provide integrated voice, data, and video services. Over

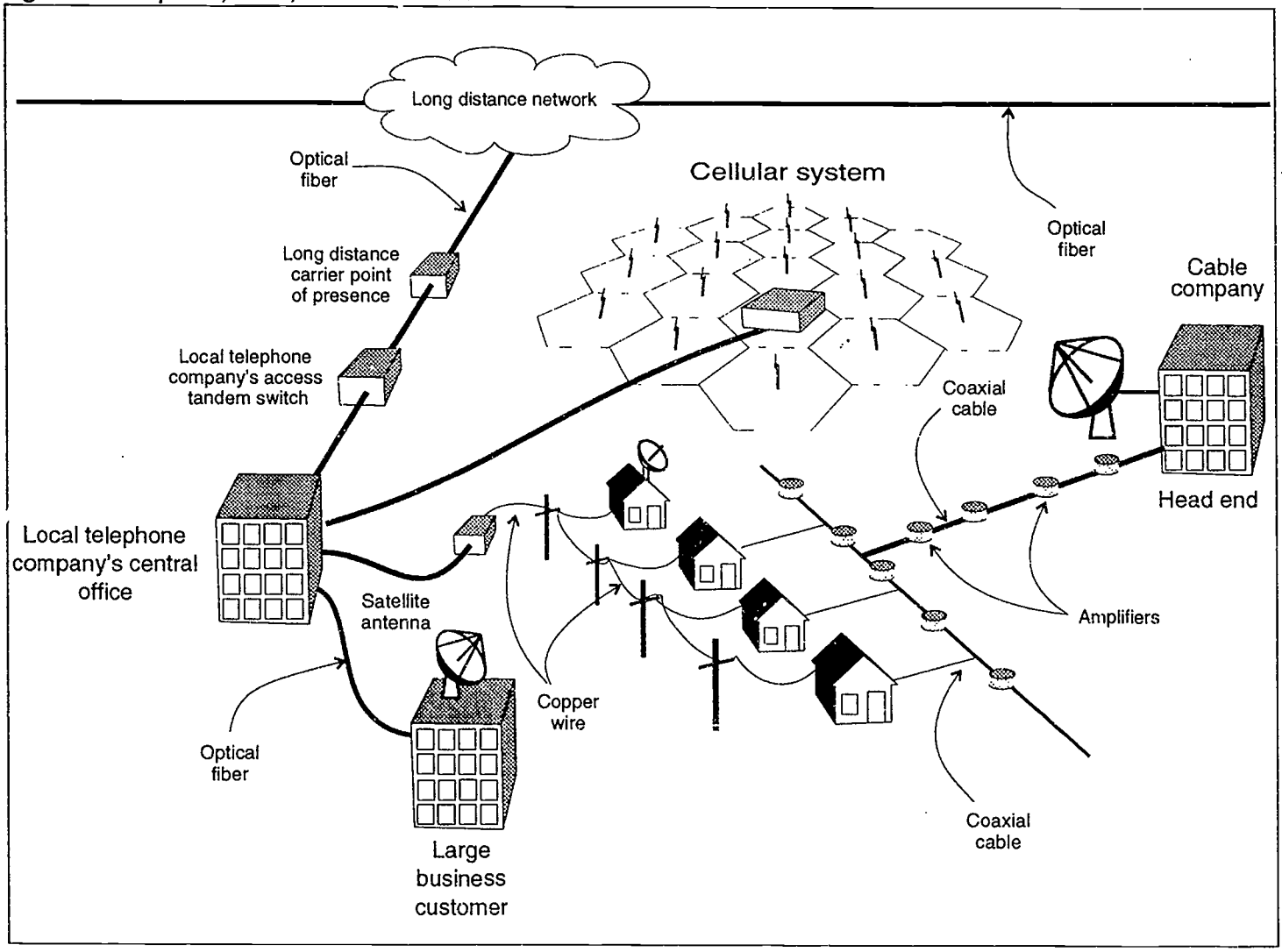
[4]An additional type of data network—the fiber optic networks used by electric power utilities to manage their power distribution systems—also exists. These networks may eventually become part of the information superhighway.

[5]Unlike the private networks developed for the exclusive use of one organization, the U.S. common carrier networks are shared-resource networks that offer communications services to public subscribers.

the years, the voice and data networks have evolved separately, with voice networks relying on circuit switching while data networks largely using packet switching techniques. Thus, a business user requiring voice, data, and videoconferencing services may have to use three separate networks—a voice network, a data network, and a videoconferencing network. The emergence of multimedia applications and the high bandwidth applications in health care, industry, education, and business are beginning to require a network infrastructure capable of supporting multiple types of information.

The basic architecture of the three types of networks is shown in figure 1.2 (see appendix II for an overview of each of these networks).

Figure 1.2: Telephone, Cable, and Wireless Networks



The communications industry is beginning to introduce several new and innovative technologies that could enable the superhighway's developers to achieve the administration's vision of the information superhighway. These technologies include

- narrowband Integrated Services Digital Network (ISDN),
- advanced signaling and intelligent networks,
- broadband ISDN (B-ISDN),
- personal communications networks, and
- broadband in the local loop.

These technologies, described in more detail in appendix III, will help provide many of the advanced services and capabilities of the information superhighway. The development of the superhighway will also require the expenditure of tens of billions of dollars to build the local broadband "on-ramps" connecting residential, institutional, and business users with the evolving superhighway.[6] Further, its users are expected to be offered viable services and information products beyond the much touted 500 channels of high-definition television.[7]

Objective, Scope, and Methodology

In light of the strategic importance of the information superhighway, we identified the socioeconomic, regulatory, and technical issues and challenges associated with the development of the information superhighway. Our previous report addressed all three areas.[8] Our objective in this report is to address in more detail the key technical issues: security and privacy, interoperability, and network reliability.

To accomplish our objective, we surveyed an extensive body of technical literature and industry journals, searched and reviewed related documents from Internet networks, and reviewed postings to various Internet news groups with interest in telecommunications and information security issues. To obtain the views of federal officials on the technical challenges related to the development of the information superhighway, we met with representatives from the Federal Communications Commission (FCC), the National Telecommunications and Information Administration, the Information Infrastructure Task Force (IITF), the National Institute of

[6]Cable Television Laboratories estimates that the replacement of the copper wire in the local loop will cost hundreds of billions of dollars.

[7]Many argue that once the industry provides the on-ramps, a rich array of services requiring interactive, broadband transmission capabilities will be developed. Others believe that the response to the view "if we build it, they will come" is "yes, but will they bring any money?"

[8]Information Superhighway: Issues Affecting Development (GAO/RCED-94-285, Sept. 30, 1994).

Standards and Technology (NIST), the National Science Foundation, the Department of Defense (DOD), the Advanced Research Projects Agency (ARPA), and the National Security Agency (NSA). We also met with representatives of the telephone, cable, and communication industry to obtain their views on technical issues related to the superhighway.

We conducted our work in Washington, D.C., and vicinity between September 1993 and October 1994, in accordance with generally accepted government auditing standards. In addition, we discussed the contents of this report with representatives of the National Telecommunications and Information Administration, IITF, FCC, NIST, DOD, ARPA, and NSA, and have incorporated their comments where appropriate.

Ensuring Security and Privacy Will Pose a Major Challenge

Much of the information that will be on the superhighway, including health care records, business documents, engineering drawings, purchase orders, or credit card transactions, will be proprietary or privacy sensitive and must be protected. As it evolves, the superhighway will become an increasingly tempting target for intruders with the technical expertise and resources to cause great harm, including insiders,[1] hackers, foreign governments conducting political and military intelligence operations, domestic and foreign enterprises engaged in industrial espionage, and terrorist groups seeking to disrupt our society or cripple our economy.[2] Unauthorized disclosure, theft, modification, or malicious destruction of such information could bankrupt a business, interrupt vital public service, or destroy lives.

Information security plays a key role in protecting computer systems, networks, and information—including voice, fax, and data communications—from harm, disclosure, or loss. Privacy depends heavily on security.[3] In essence, there is little or no privacy protection afforded by poorly secured information systems and networks. While privacy-enhancing legislation, regulations, and management practices play an important role in reducing the threat to individual privacy, it is security technology that will provide many of the safeguards.[4]

Significant effort will be needed to define, develop, test, and implement measures to overcome the security challenge posed by the increasing complexity, interconnectivity, and the sheer size of the evolving superhighway. These measures include identifying the superhighway's security and privacy requirements and developing tools and techniques to satisfy the requirements.

The federal government, because of its extensive experience and expertise in developing secure networks, is addressing selected aspects of security and privacy. However, critics of federal involvement argue that the current federal strategy represents a danger to civil liberties and that individuals

[1]Many violations of information safeguards are perpetrated by trusted personnel who engage in unauthorized activities or activities that exceed their authority. These insiders may copy, steal, or sabotage information, yet their actions may remain undetected.

[2]Economic Espionage: The Threat to U.S. Industry (GAO/T-OSI-92-6, Apr. 29, 1992).

[3]Privacy is the state of being free from unsanctioned intrusion; a condition in which an individual can determine when, how, and to what extent information about him or her is collected, used, and communicated to others.

[4]Information Security and Privacy in Network Environments, Office of Technology Assessment, Washington, D.C. September 1994.

should be free to choose the technical means for achieving information security. As a result, the challenge will be establishing a reasonable level of consensus among the major players—the government, the computer and communications industry, the business community, and civil liberty groups—on how to ensure information security and privacy on the information superhighway.

Networks and Computer Systems Are Increasingly Vulnerable to Attacks

The vulnerability of interconnected computer systems is periodically highlighted by attacks on the thousands of computer systems connected to the Internet. These attacks provide an important lesson. The Internet—the world's largest network of networks—has many of the same attributes that will eventually be found in the information superhighway. The information superhighway may not only share similar vulnerabilities, but it may face similar, albeit greatly magnified, threats.

Two major security incidents affecting the Internet illustrate the risk to the evolving information infrastructure. On November 8, 1988, thousands of computers connected to the Internet were attacked by a worm.[5] While the worm did not damage or compromise data, it did deny service to thousands of users working at the nation's major research centers. We found that a number of vulnerabilities facilitated this attack, including the lack of a central focal point to address Internet-wide security problems; security weaknesses at host computer sites; and problems in developing, distributing, and installing software patches to operating system software.[6] In response to this incident, the Advanced Research Projects Agency established a Computer Emergency Response Team to assist the Internet community in responding to attacks. Several federal agencies and private-sector organizations also established additional computer emergency response teams coordinated by NIST.

Five years later, in January 1994, intruders again exploited similar weaknesses. This time, the attack was more serious. The intruders gained access to a number of hosts (computer systems) linked to the Internet. The intruders then installed software that captured user names, passwords, and hosts' addresses for Internet traffic terminating at, or passing through, the attacked sites. In addition, they installed two Trojan

[5]Worms are self-contained programs containing malicious code that copy versions of themselves across electronically connected nodes.

[6]Computer Security: Virus Highlights Need for Improved Internet Management, (GAO/IMTEC-89-57, June 12, 1989).

horse programs,[7] one program to provide back-door access for the intruders to retrieve the captured passwords, and a second program to disguise the network monitoring process. With this information, the intruders could access 100,000 Internet accounts.[8] The Department of Defense reported that the attacks compromised a major portion of the international commercial networks as well as major portions of the unclassified Defense information infrastructure. Defense functions affected by the attacks included ballistic weapons research, ocean surveillance, and the military health care systems.

Security Measures Are Critical to Minimizing Risk

Reducing the frequency and damage of attacks against the national networks will require a significant effort to provide the tools and resources necessary for the development and deployment of infrastructure-wide security services. These services include

- identification and authentication—the ability to verify a user's identity and a message's authenticity,
- access control and authorization[9]—the protection of information from unauthorized access,
- confidentiality—the protection of information from unauthorized disclosure,
- integrity—the protection of information from unauthorized modification or accidental loss,
- nonrepudiation—the ability to prevent senders from denying they have sent messages and receivers from denying they have received messages, and
- availability—the ability to prevent denial of service, that is, to ensure that service to authorized users is not disrupted.

Cryptography[10] will play a key role in the development of five of the six security services for the information superhighway. It helps, through password encryption, to improve identification and access control; it protects confidentiality and data integrity by encrypting the data; and finally, it improves, through encrypted electronic signature and related means, nonrepudiation services.

[7]A Trojan horse is a program that conceals malicious computer code. Typically, a Trojan horse masquerades as a useful program that users would want or need to execute. It performs, or appears to perform, as expected, but also does surreptitious harm.

[8]Computer Incident Advisory Capability team, Department of Energy.

[9]Authorization involves two steps—identification and authentication.

[10]Cryptography is a technique for transforming ordinary text (plaintext) into unintelligible ciphertext through encryption.

Two basic types of cryptographic systems exist: secret key systems (also called symmetric systems) and public key systems (also called asymmetric systems).[11] In secret key cryptography, two or more parties use the same key to encrypt and decrypt data. As the name implies, secret key cryptography relies on keeping the key secret. If this key is compromised, the security offered by cryptography is eliminated. The best known secret key algorithm is the Data Encryption Standard. It is currently the most widely accepted, publicly available symmetric cryptographic algorithm. Secret key systems also require that a secure communications channel be established for the delivery of the secret key from the sender to receiver. Such a secure, nonelectronic communications channel for the distribution of secret keys is costly to establish and maintain.

Unlike secret key cryptography, which employs a single key shared by two or more parties, public key cryptography uses a pair of matched keys for each party. One of these keys is public and the other private. The public key is made known to other parties—mainly through electronic directories—while the private key must be kept confidential. Thus, under the public key system, there is no need to establish a secure channel to distribute keys. The sender encrypts the message with the recipient's freely disclosed, unique public key. The recipient, in turn, uses her unique private key to decrypt the message.

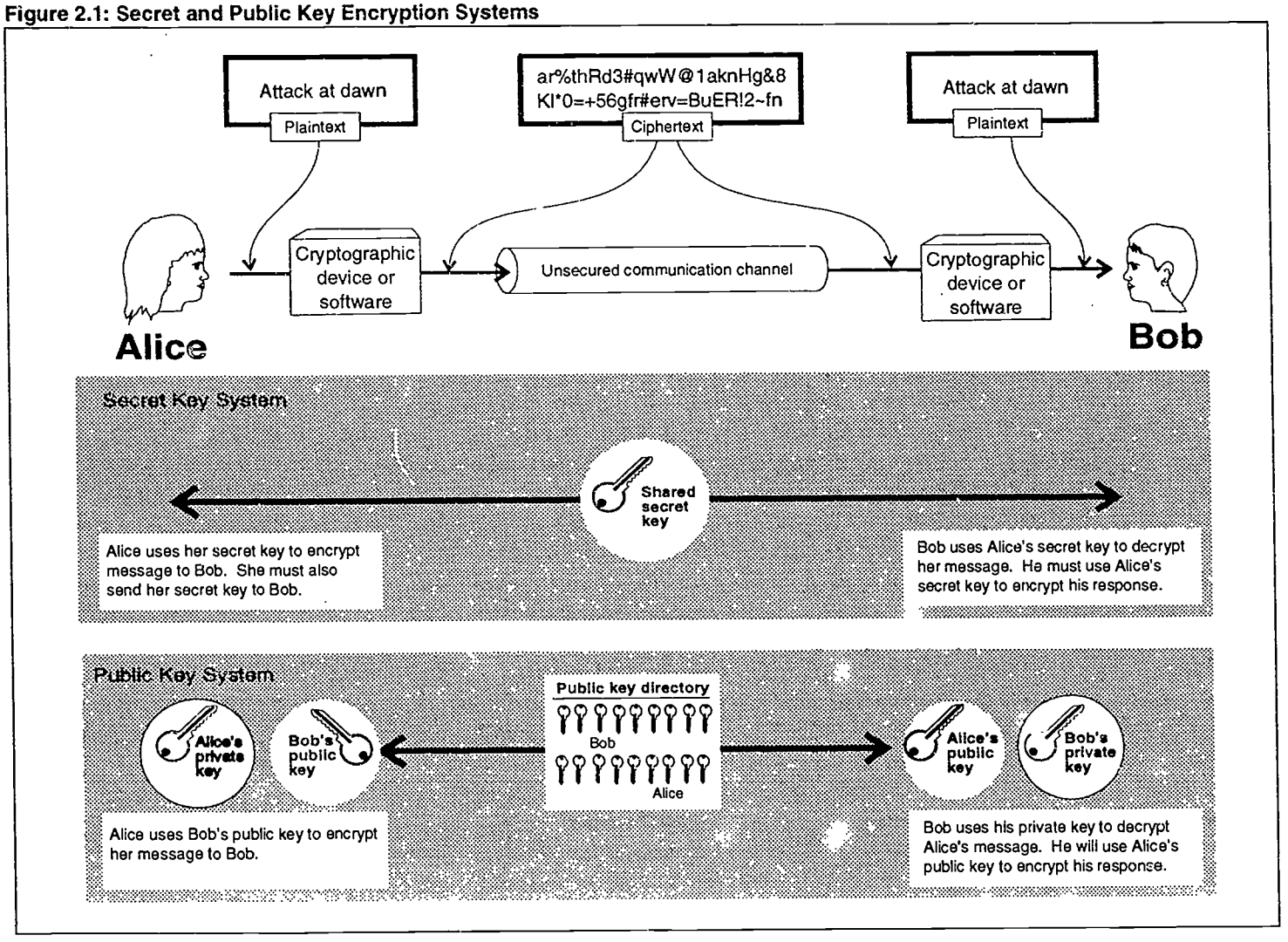
Public key cryptography also enables the user to produce an electronic signature. The user encrypts the signature using the private key, which, when decrypted with the public key, provides verification that the message originated from that user. The best known public key algorithm is the Rivest-Shamir-Adelman algorithm.[12] The Pretty Good Privacy software, which implements the Rivest-Shamir-Adelman algorithm, is probably one of the best known public key cryptographic systems.[13] Figure 2.1 highlights the principal features of the secret and public key cryptographic systems.

[11]A key is a unique sequence of letters, numbers, or combination of both that is used to encrypt and decrypt messages.

[12]Rivest-Shamir-Adelman is a public key algorithm used for both encryption and authentication; it was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adelman.

[13]The Pretty Good Privacy is a public key cryptographic system developed by Philip Zimmerman.

Figure 2.1: Secret and Public Key Encryption Systems

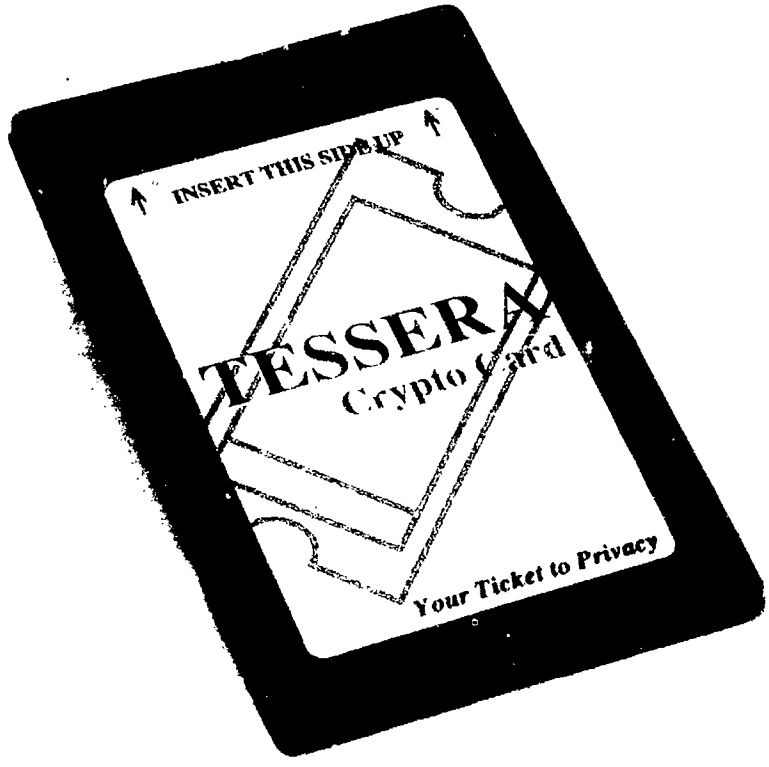


A host of related security technologies, including computer memory cards, will also play an important role in securing the information superhighway. Computer memory technology uses a credit-card-size electronic module to store digital information that can be recognized by a network or a host system. Figure 2.2 shows a computer memory card—the Tessera Crypto Card—developed by the National Security Agency.[14] The Tessera Crypto

[14]The Tessera crypto card, based on the Personal Computer Memory Card International Association Industry standard, was recently renamed Fortezza. The card is a key element of the Department of Defense's Multilevel Information Systems Security Initiative.

Card is a small, portable cryptographic module that provides high-speed authentication and encryption services.

Figure 2.2: Tessera Crypto Card



Federal Role in Security and Privacy Is Subject to Debate

Federal involvement in communication security is fueling a debate over the federal role in regulating the development and use of encryption and communications technologies. Critics of federal involvement, such as the Electronic Frontier Foundation—a public interest organization focused on protecting civil liberties in digital environments—believe that government control of encryption technologies and their implementation represents a danger to civil liberties, and that individuals should be free to choose the technical means for meeting their security requirements. Others, including NIST and Defense officials, maintain that the federal government's participation and guidance in securing the information superhighway may be needed for several reasons. First, the government is a major consumer

of telecommunications services and has unique national security and law enforcement needs that must be addressed. Second, the government, and particularly the Department of Defense, has considerable experience in the areas of computer and communications security. Defense, the developer and operator of the world's largest secure communications network, could provide expertise needed to help develop the superhighway's security architecture. The need for such an architecture was underscored by a recent study which noted that it is "imperative to develop at the outset a security architecture that will lay the foundation for protections of privacy, security, and intellectual property rights—safeguards that cannot be supplied as effectively on an add-on basis."[15]

Since the invention of the telegraph and telephone, intelligence and law enforcement agencies have conducted legal intercepts of communications both here and abroad. In general, these agencies used technically simple intercepts that targeted unprotected communications. However, the emergence of digital technologies and the increased availability of sophisticated encryption tools has dramatically eroded the government's electronic intelligence and analysis capabilities. The proliferation of digital communications is making wiretapping increasingly difficult, while robust encryption prevents third parties, including law enforcement and intelligence agencies, from deciphering and understanding intercepted messages.

The administration, after coordination with the Congress, industry, and public advocacy groups, has developed a strategy designed to preserve the government's ability to conduct electronic surveillance, wiretapping, and analysis of voice and data communications between criminals, terrorists, drug dealers, and foreign agents. This strategy includes

- a major new federal cryptography initiative known as the Key Escrow Standard (popularly known as the "Clipper chip" program),
- the Communications Assistance for Law Enforcement Act requiring the information industry to provide "built-in" wiretapping support in its digital communications systems, and
- restrictions on the export of encryption technology.

[15]Realizing the Information Future, National Research Council, National Academy Press. Washington, D.C.: 1994, p. 5.

Key Escrow Initiative Intended to Improve Communication Security

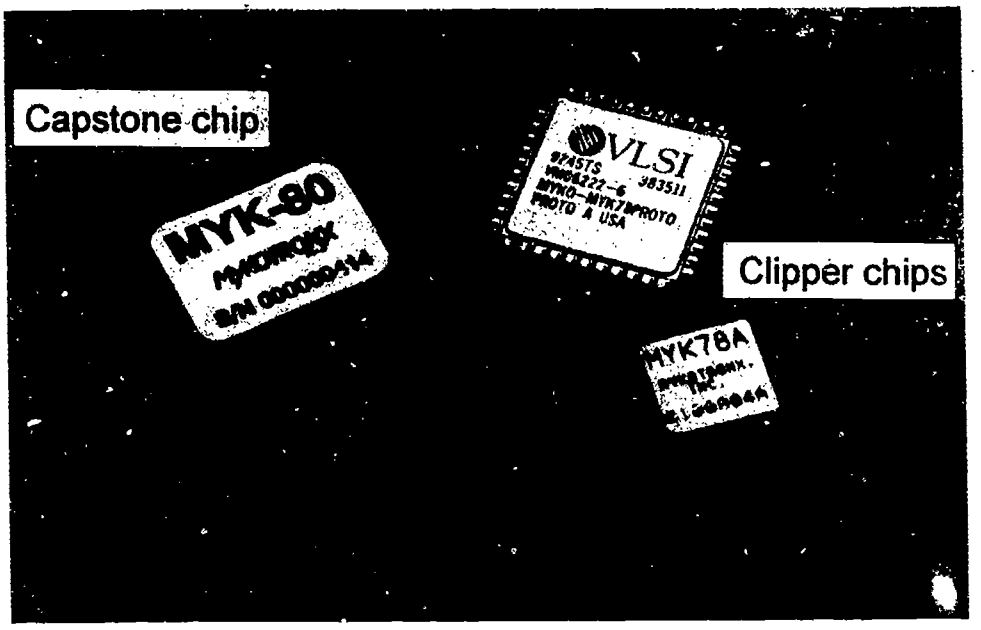
The Key Escrow initiative is a voluntary program to improve the security and privacy of telephone communications in the private sector while meeting the legitimate needs of law enforcement. In essence, the initiative is the government's attempt to preempt the threat posed by sophisticated encryption capabilities by offering the industry a relatively inexpensive, albeit government-controlled, hardware-based encryption system capable of providing secure voice, fax, and data services. To ensure that law enforcement agencies are able to understand Clipper-encrypted voice communications, the private encryption keys assigned to each individual Clipper chip are to be escrowed with the government. These keys will be made available to law enforcement agencies for court-ordered wiretaps.

The Clipper chip, developed by NSA, is a microcircuit incorporating a classified encryption algorithm known as Skipjack.[16] The chip, and its close relative, the Capstone chip, contain a unique key that is used to encrypt and decrypt messages, programmed by the escrow agents.[17] This unique key is then split into two components and delivered to two federal agencies—or escrow agents—for safekeeping. When federal authorities encounter Clipper chip encrypted voice or Capstone chip encrypted data communications during the course of court-authorized wiretapping, they may obtain the unique key necessary for the decryption of the wiretapped communications from the escrow agents. Figure 2.3 shows a Capstone chip and three prototypes of a Clipper chip.

[16]The power of the Clipper chip technology is highlighted by comparing it to earlier voice encryption devices. For example, in the early 1940s, the administration asked scientists at the Bell Telephone Laboratories to develop a telephone scrambler that would allow Winston Churchill and President Roosevelt to have secure conversations. Code named "Sigsaly," this transatlantic scrambler needed, at the London end, not only a five foot high intermediate scrambler cabinet, but also over 30 seven foot tall relay racks weighing eighty tons, 72 different radio frequencies, a large air-conditioned room, and 30 kW of energy to encipher one short conversation (The Cabinet War Rooms, Imperial War Museum, London, 1994).

[17]The Clipper chip is designed to encrypt voice transmission; the Capstone chip is designed to encrypt data and video transmission.

Figure 2.3: The Capstone and the Clipper Chips



Source: National Security Agency.

In April 1993, the President directed the Attorney General to (1) request manufacturers of communications hardware that incorporates encryption to install the Clipper chip in their products, and (2) designate two government organizations as "key escrow" holders. The President also directed the Secretary of Commerce to initiate, through NIST, a process to develop federal key escrow encryption standards. Despite strong industry opposition,[18] the administration reaffirmed its 1993 directive and instructed the Secretary of Commerce to approve the Clipper chip as a voluntary national standard for encrypted telephone communications. In February 1994, NIST formally approved the new standard. At the same time, the Attorney General designated NIST and the Automated Systems Design Division of the Department of the Treasury as the key escrow agents.

Critics of the Key Escrow initiative argue that NSA's refusal to declassify and publish the Skipjack encryption algorithm raises the possibility that

[18]In July 1993, NIST asked industry to comment on the proposed standard. Of the 320 respondents, only 2 supported the proposed standard.

the algorithm may have a built-in "trap door."[19] Such a trap door would allow intelligence agencies to decrypt Clipper and Capstone encrypted communications at will, without obtaining the private keys from the escrow agents.[20] The critics also note that since robust encryption technology is available both in the U.S. and abroad, there is no incentive for domestic and international industry or private citizens to adopt the Clipper/Capstone technology.

The misgivings about the Key Escrow initiative were also shared by the Computer System Security and Privacy Advisory Board.[21] In its June 4, 1993, resolution, the Board stated that the administration has not (1) provided a convincing statement of the problem that Clipper attempts to solve, (2) considered other escrow alternatives including the designation of a third, non-government escrow agent, and (3) fully examined the legal and economic implications of the Clipper chip initiative. The Board recommended that the Key Escrow encryption technology not be deployed beyond current implementations planned within the Executive Branch until the significant public policy and technical issues inherent with this encryption technique are fully understood. The Congress asked the National Research Council to conduct a comprehensive study of national cryptography policy and submit, within 2 years, a report to the Secretary of Defense.[22] In December 1993, the Board endorsed the proposal, noting that the study should be conducted as quickly as possible.

In July 1994, the administration reaffirmed its commitment to the Key Escrow scheme in general, and to the use of the Clipper chip for telephone communications in particular. It also offered a compromise on the development of the Capstone chip for computer and video networks. Specifically, the administration said that it understood the concerns that industry has regarding the Capstone chip and welcomed the opportunity to work with industry to design a more versatile, less expensive system. NIST and the information security industry have now initiated a joint effort to explore alternative approaches. Such alternative key escrow schemes

[19]A trap door is a hidden software or hardware mechanism that allows systems controls to be circumvented. Software developers often introduce trap doors in their code to enable them to reenter the system later and perform certain functions.

[20]On more than one occasion, administration officials, including the Deputy Director of NIST, have testified before Congress that the Skipjack algorithm does not incorporate a trap door mechanism.

[21]The Board, composed of representatives from the computer and telecommunications industry, independent experts in telecommunications, and federal employees, was established by the Computer Security Act of 1987 to advise the Secretary of Commerce and the Director of NIST on security and privacy issues.

[22]Public Law 103-160, Section 267.

would be implemented in software, firmware, or hardware, or a combination thereof; would not rely on a classified algorithm; would be voluntary; and would be exportable.[23]

Legislation Enacted to Facilitate Digital Wiretaps

To address concerns about the potential loss of wiretapping capability due to the rapid deployment of digital communications,[24] in October 1994 the Congress enacted the Communications Assistance for Law Enforcement Act.[25] The act requires common carriers to ensure that they posses sufficient capability and capacity to accommodate law enforcement's wiretapping needs. Specifically, the act requires that telecommunications carriers develop the capability to expeditiously isolate the content and call-identifying information of a targeted communication and enable the government to access targeted communication at a point away from the carrier's premise. The act requires the government to reimburse carriers for all reasonable costs associated with complying with the act's requirements. Critics of the act—including the Electronic Frontier Foundation—argue that it further erodes communication privacy, and that the Federal Bureau of Investigation has not adequately documented its need for sophisticated digital wiretap capability.

Federal Government Restricts the Export of Encryption Technology

Many of the U.S. encryption technologies, whether developed commercially or by the government, are subject to export controls. The Departments of State and Commerce share responsibility for controlling the exports of these technologies.[26] However, computer industry representatives view the encryption export controls as counterproductive and economically damaging. For example, the representatives noted that because robust, sophisticated encryption technologies, including technologies on the U.S. Munitions List, are widely available in foreign markets, the export controls are reducing their international sales.[27]

Our brief search of foreign Internet sites confirms industry's assertion that sophisticated encryption software is widely available to foreign users. For

[23]Letter from Vice President Al Gore to the Honorable Maria Cantwell, House of Representatives, July 20, 1994.

[24]Electronic Surveillance: Technologies Continue to Pose Challenges (GAO/T-AIMD-94-173, Aug. 11, 1994).

[25]Public Law 103-414.

[26]Certain encryption products are placed on the U.S. Munitions List. These products require a munitions license for export to foreign countries.

[27]Communications Privacy: Federal Policy and Actions, (GAO/OSI-94-2, Nov. 4, 1993).

example, we found that a number of European Internet sites are offering U.S.-made encryption software. In less than two hours, we identified several European sites offering the Pretty Good Privacy software, obtained it from an Internet site in Great Britain, installed the software on our computer, and encrypted a message (shown in figure 2.4).

Figure 2.4: Message Encrypted With the Pretty Good Privacy Encryption System

Plaintext Message With Encrypted Signature

—BEGIN PGP SIGNED MESSAGE—

Our brief search of foreign Internet sites confirms industry's assertion that sophisticated encrytpion software is widely available to foreign users.

—BEGIN PGP SIGNATURE—
Version: 2.6

iQCVAgUBLkEE7iR4seyvySXFAQGqJAQAmTge8TslZTiXIt4cgrBr6qG
ZZfMkEvIm IVFVMP41xWlME+uzJiKWIydWUpXHFi0EzR337I3Nx54N
JyoSoHE1zuAuLR0sVq+7 QMNFaHby2s0HAgByUH6SEHAyCyQZ1UB
m+8Unrb2tsgfNIf6nQfW6z0F4TUV5QNpL bXQiU6JuyEI=
=ErFY

—END PGP SIGNATURE—

Encrypted Message

—BEGIN PGP MESSAGE—
Version: 2.6

hIwCZXmEuMepZt0BBACl0wb3FtNerMXZlAPAVWkaVP9tes44j98sJREVwg
COMLFr IIhvJrm7KA1wiGdHTQXLvdyJNm3PHAXZqKz31eA/WeJRO/cFf1jT
Hx0cCg5Q/buY SdewGCl8gqGG6TyQujBPw73qz93uUSA3/jpzhjI3EiE9sSaK
i6Qjd1KV14o1nYSM AiR4seyvySXFAQP9Gogj63PMFnYiHSV8pPk7tUcwjp
FNXan6pVViwt6JowSbPtUP ib4p6XfI6D0ZjzhlJ9Jwd4A9jpD91tRn5kUnz2D
YNS1ZtJIasWYUMTBYy/lm/QMC 7qaIFKpqjVMOBkiy9Tbz3ToShS7ae2ac
OnWovJkjBjP70CfGJLo0AsEz+1mmAAAB Tb/6nhH7IAN+9cQ7gEfl0jJKuK/
uRdVHemACEBLBbIqK2ELog+9hMfRA4eV4vROK 0I9A2wEMQg4DPORS
wrUVQlyehGPQok86EMI1fG0t7bH/SjrdAg/zS1HbwtaWQM51 g9+sfFCiktD
kaETdUZjs+zCPhlS5jy6MpOcvt9x3hkwv50iHpOtfjZ3zHUml3827 +SCJJOA
x4aZ50blBoeEQJHC0/NPPb++A0cCNS5rvktvgG/jFN1po.VHex/3301DY dni
hIcs0r33nWAhCG1jIH6hiufUvoXKxpSWX+KUXROS1HZYo84/541g2O6pfk
dQO 3l0yJZlJRL9xPp0nfZC6MaHEGPnMZRqoF3gB7xbU5PUUOrkXIMoq8
tzVOxmAJpwq R9DKkWht356VRVBjkFlQ9pIZTuQ/JBcToWrgk56i/xTWldcb
ks4S75dbreYB1sM= =YCVl

—END PGP MESSAGE—

Achieving Interoperability Is a Critical Goal

Interoperability—the ability of two or more components of a system or network to interact with each other in a meaningful way—is a key goal of the information superhighway. However, full interoperability among the thousands of networks, communications devices, and services that will comprise the information superhighway will be difficult to achieve. To do so, governments, industry, and standards-setting organizations must agree on well-defined international standards for rapidly advancing communications technologies, while manufacturers and service providers need to provide products and services conforming to these standards. However, the telecommunications industry is already deploying, or plans to deploy, a host of technologies and services that are based on ill-defined, anticipatory, or competing standards. To address this dilemma, the federal and private sectors have initiated interoperability efforts, including the assessment of various "open network" architectures.[1]

Interoperability Will Be Difficult to Achieve

Interoperability will define the information superhighway. Without interoperability, the information superhighway will be fragmented into thousands of poorly integrated communications networks providing a bewildering choice of incompatible services. While policymakers, public interest groups, and industry agree that interoperability is a key requirement, they also agree that it will be difficult to achieve among the thousands of communications networks, computers, databases, and consumer electronics that will comprise the information superhighway. As discussed in chapter 1, the existing infrastructure suffers from significant interoperability problems.

New Technologies Being Deployed Are Based on Ill-Defined, Anticipatory, and Competing Standards

Because of competitive pressures, the desire to provide new capabilities, and a belief that the traditional standards-setting process is unable to keep up with the fast pace of technological change, industry is deploying, or is planning to deploy, a host of new technologies and services. However, many of these technologies and services are based on ill-defined, anticipatory, or competing standards, thereby further complicating efforts to achieve interoperability.

The effects of deploying new technology based on ill-defined standards is illustrated by the implementation of the ISDN. ISDN is an end-to-end digital network evolving from the existing telephone network. It is viewed as the first step in the conversion to a fully digital network. However, the initial

[1]The National Research Council defines an open network as one that is capable of carrying information services of all kinds, from suppliers to customers, across network service providers of all kinds, in a seamless, accessible fashion.

deployment of ISDN resulted in the proliferation of "island" ISDN services that could not interoperate because the ISDN standards provided only a broad outline and lacked enough detail to ensure that all implementations would be identical. For example, ISDN users in New York and New England are unable to communicate data with ISDN users in the middle atlantic states. To alleviate the ISDN interoperability problems, the industry announced a plan to establish a consistent interface that would provide interoperability between local telephone companies, long distance telephone companies, and equipment manufacturers.

The deployment of the Asynchronous Transfer Mode (ATM) services provides an example of a technology deployed based on anticipatory standards. The broadband ISDN (B-ISDN) technology, which is expected to lay the foundation for the superhighway's interactive, high-speed digital communications infrastructure, will rely on ATM/SONET optical fiber networks.[2] However, critical ATM standards including global routing and addressing, resource management, multicast,[3] and network management remain undefined. The industry is also developing products and services in the absence of less visible, but equally important standards, for data display and exchange, accounting and billing, network addressing and naming, and telephone number portability (see appendix IV).

The introduction of competing technologies is highlighted by the deployment of digital cellular systems. Digital cellular systems are viewed as a key component of the evolving personal communications networks. While digital systems will offer dramatically better performance than their analog counterparts, their near-term value in serving as a key link in the emerging B-ISDN network is reduced by compatibility problems. There are three principal digital cellular standards—the U.S. standard, known as the North American Dual-Mode Cellular System; the European standard, known as Global System for Mobile Communications; and the Japanese Digital Cellular standard. Although all three standards are based on the time division multiple mode access technique,[4] they are not interoperable.

[2]ATM is a fast packet switching technology utilizing small, fixed-size cells. Synchronous Optical Network (SONET) is the U.S. implementation of an international synchronous digital hierarchy standard for optical carrier networks.

[3]Multicast is a variant of broadcast, where information can be sent to selected recipients instead of all subscribers of a particular communications systems.

[4]A digital encoding scheme that allows users to simultaneously transmit on the same frequency by allocating each user a discrete time slot.

The Federal and Private Sectors Have Initiated Efforts to Address Interoperability

While the key players—the federal government, the computer and communication industries, and various user groups—appear to agree on the need for a fully interoperable information superhighway, there is no agreement yet on how it should be achieved. The principal federal organizations focused on superhighway interoperability include NIST and the National Research Council's Computer Science and Telecommunications Board.[5] The overall coordination of federal interoperability efforts is being examined by IITF's Technology Policy Working Group. In the private sector, the FCC is working with industry to ensure the interoperability of selected technologies deployed in public networks. Industry has also established a consortium for the development and testing of superhighway applications.

National Research Council Advocates High-Level Architecture to Guide Interoperability Efforts

One promising approach to the planning for interoperability is to develop a high-level architecture—or framework—of the superhighway. This approach was advocated by a recent National Research Council report that presented a vision of the superhighway based on an open data network concept.[6] Under this concept, the superhighway must be

- open to users: it does not force users into closed groups or deny access to any sector of society, but permits universal connectivity, as does the telephone system,
- open to service providers: it provides an open and accessible environment for competing commercial or intellectual interests, including information providers,
- open to network providers: it makes it possible for any network providers to meet the necessary requirements to attach and become a part of the aggregate of interconnected networks, and
- open to change: it permits the introduction of new applications and services over time; it also permits the introduction of new transmission, switching, and control technologies as these become available.

This concept, expressed as a high-level network architecture, could provide a set of specifications to guide the detailed design of the information superhighway. Without such a framework, the pieces of the emerging superhighway may not fit together. The IITF's Technology Policy Working Group is planning to examine the open data network concept and

[5]The federal interagency High Performance Computing and Communications program is also addressing a wide range of network interoperability issues.

[6]Realizing the Information Future, National Research Council, National Academy Press. Washington, D.C.: 1994.

its applicability to various industries, including cable television, broadcasting, communications and computer.

Industry Responds to Interoperability Problems

In an attempt to improve interoperability, the Network Operation Forum of the Alliance for Telecommunications Industry Solutions established the Internetwork Interoperability Test Plan Ad Hoc Committee. However, the committee's effort was limited to solving problems with the Signaling System 7 (SS7)[7] switching systems. The requirements for intranetwork, product-to-product, and stand-alone equipment modeling and testing were considered to be outside of the committee's charter. Other aspects of existing networks such as interoperability testing requirements of newer technologies were also not addressed. So far, the committee has developed scenarios designed to test the interoperability of SS7 systems.

[7]SS7 is an international common-channel signaling system.

Network Reliability Is Emerging as a Key Challenge

Ensuring the reliability[1] of the information superhighway will be essential. The public and private sectors are increasingly dependent on the existing telecommunications networks, which will be the foundation of the information superhighway, to meet their business needs. Yet recent outages on these networks have raised concerns and caused economic losses. Moreover, new technologies and industry trends will likely increase network vulnerability, making reliability of the superhighway a key challenge. The government and industry have recently taken several steps to address reliability, including the formation of the Network Reliability Council and the Alliance for Telecommunications Industry Solutions.

Reliability of the Superhighway Will Be Essential

In providing critical commercial and personal services, the superhighway will require a highly reliable network. The nation is already dependent on the existing networks, which will provide the underpinning for the superhighway. For example, in addition to conventional telephone services, computers are networked together, facsimile machines provide almost instant access to images and documents, and teleconferencing and videoconferencing have emerged as substitutes for travel. The number of electronic transactions conducted over these networks is enormous. For example, the value of the telephone transactions that take place daily on Wall Street exceeds one trillion dollars. Similarly, the Federal Aviation Administration relies on the public network to transmit air traffic control information between individual airports.

Public telephone networks are also being increasingly relied upon for emergency services. For example, the telephone has replaced fire alarm boxes as the primary method for reporting fires. Emergency 911 service can be obtained from personal or public pay phones. Telephones are also used to report medical emergencies requiring emergency medical technicians, and burglaries and domestic problems requiring responses from the police. Enhanced 911 service, available in many locations, is even capable of automatically routing the emergency call to a public service answering point, the facility in charge of answering calls and dispatching appropriate services in the caller's area. The system also searches phone company databases to determine and report the caller's location and telephone number to the dispatcher.

[1]Reliability is the probability that a system will not fail over a given period of time and under specified conditions. It is based on the combined reliability of all of the components that make up the system, their interconnections, and the environment in which the system operates.

Recent Network Outages Have Raised Concerns and Caused Economic Losses

While the public and private sectors are becoming more dependent on networks, a growing number of major outages have raised concerns, triggered losses of service, potentially risked lives, and affected the economy. Several of these outages are highlighted below.

May 8, 1988: More than 500,000 business and residential customers lost telephone service due to a fire at the Hinsdale, Illinois, central office. During the following two weeks, approximately 3.5 million calls were disrupted. Hospitals with centrex service in the affected area could not make calls from one floor to another. Twenty percent of the departing flights from O'Hare International Airport were canceled and flights from other airports around the country had to be rescheduled. In a study of the Hinsdale outage, the University of Minnesota concluded that the cost of network failures to airlines could be between $2 and $3 million per hour and investment bankers could lose up to $5 million per hour.

Jan. 4, 1991: Maintenance workers in a cable vault in New Jersey accidentally cut an optical fiber transmission line that provided service to lower Manhattan. Sixty percent of the calls into and out of the city were disrupted for eight hours. The New York Mercantile Exchange and the Commodity Exchange had to shut down operations. Voice and radar systems that are used to control air traffic from facilities in New York, Washington, and Boston were disabled for five hours.

Sept. 17, 1991: Through a power sharing arrangement with New York's Consolidated Edison, AT&T agreed to use its own power when Consolidated Edison's facilities were heavily loaded.[2] On this particularly warm day in September, AT&T switched to its own power. Batteries designed to meet the initial instantaneous power demand performed as intended. However, alarms that were intended to inform technicians to start the facility's diesel generator had been manually disabled. When the batteries discharged, all telephone transmission systems in the facility shut down and voice and data communications controlled by the facility failed. Voice and data communications between the New York, Boston, and Washington Air Route Traffic Control Centers stopped. Three New York area airports closed for several hours. Flights destined for New York were either delayed or canceled. Air traffic at Boston was severely disrupted and delays occurred nationwide. More than 1,174 flights were canceled or delayed and approximately 85,000 passengers were affected. The day after the phone outage, flight schedules were still disrupted because aircraft were not at the right airports for the scheduled morning flights.

[2]Wall Street Journal, December 12, 1991.

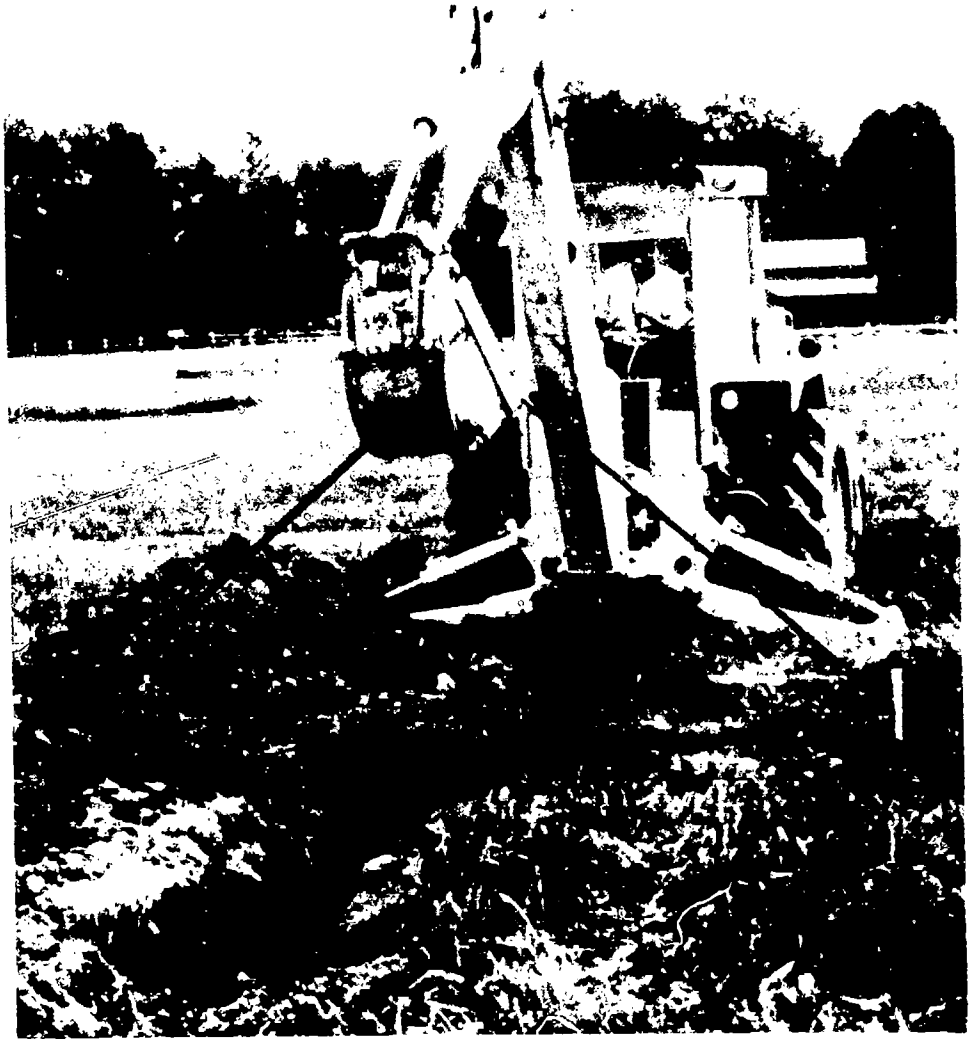
Sept. 10, 1993: A road crew boring holes for highway road signs in Ohio cut a high-capacity fiber-optic cable belonging to MCI.[3] The cable, which carries most of the company's east-to-west traffic, was repaired in about seven hours. However, millions of residential and business customers were unable to make coast-to-coast calls during that period.

March 15, 1994: During the early morning hours a fire broke out in Pacific Bell's Los Angeles central office known as the Madison Complex. Before complete service was restored, almost 17 hours later, approximately 395,000 customers may have been affected and over 5 million calls were blocked.

Cable cuts, a source of major outages, occurred 160 times during the period between March 1, 1992, and February 4, 1993, with 93 (58 percent) of them caused by "dig-up" incidents, such as the one illustrated in figure 4.1. The average time needed to restore service after a cable cut was 5.2 hours with a maximum of 21.4 hours. The average time required to repair a fiber cable cut was 14.2 hours with a maximum of 97.5 hours.

[3]Wall Street Journal, September 13, 1993.

Figure 4.1: Fiber Optic Cable "Dig-Up" Accident



Source: AT&T Technology Magazine

On February 13, 1992, the FCC instituted mandatory outage reporting requirements for outages that affect more than 30,000 customers for

durations lasting 30 minutes or longer. As of June 1994, more than 314 outages were reported. The calculation of the cost of an outage is difficult because of the variety of users that could be affected.

New Technologies, Network Growth, and Complexity Will Likely Increase Network Vulnerability

The deployment of advanced technologies, such as intelligent network architectures, common channel signaling, integrated services digital network, broadband transport facilities, customer control, and user-programmability, is increasing network complexity and vulnerability. The new technologies, described in appendix III, are also allowing network designers to concentrate more traffic into larger and fewer switches, and to rely on fewer higher capacity fiber optic cables to transmit hundreds of thousands of telephone calls. Failure of any of these high-capacity elements could be potentially devastating.

As the information superhighway grows, the number of networks and service providers is also expected to grow. Telecommunications consumers will increasingly acquire services from combinations of suppliers' products, service providers, and network providers. Increasing network complexity will make it more difficult to isolate and correct problems.

The Government and Industry Are Taking Steps to Address Reliability

In 1991, the FCC, concerned about the spate of telephone network outages that affected a large number of subscribers on both the east and west coasts, established the Network Reliability Council. The council's goal was to bring together leaders of the telecommunications industry, telecommunications experts from academia, and consumer organizations, to explore and recommend measures that would enhance network reliability. Members include the executive officers of most of the major U.S. telephone companies, principal equipment suppliers, long-distance companies, consumer organizations, corporate and federal user representatives, and state regulatory agencies.

The council established a steering committee and seven focus groups to deal with the key problem areas—signaling network systems, digital cross-connect systems, fiber cable cuts, fire prevention, enhanced 911 service, power systems, and switching systems (with a focus on software). The groups formulated recommendations for developing and implementing countermeasures to reduce the number of outages; monitoring the results; and modifying, as necessary, the countermeasures. The commission is now looking at these recommendations and

considering regulations that would require the carriers and equipment suppliers to implement them.

In 1994, the Network Reliability Council restructured and created four focus groups. The first group will concentrate on network reliability; the second will examine reliability issues arising from expanded interconnection of networks; the third will study network technology and examine reliability concerns related to providing telephone service through cable, satellites, and wireless systems; and the fourth group will study the reliability of critical services, including 911, Federal Aviation Administration, military, and government.

The Alliance for Telecommunications Industry Solutions—a private sector organization—was formed to promote the timely establishment of telecommunications standards and operational guidelines. Its members include representatives of local exchange carriers, interexchange carriers, enhanced service providers, manufacturers, vendors, and end users who participate in a number of sponsored committees.

The alliance also sponsors the Network Operations Forum, a group of telecommunications industry access providers and customers who meet periodically to identify national operations issues involving the installation, testing, and maintenance of access services. In July 1991, the alliance began focusing on the area of network reliability. One of the forum's subcommittees has developed traffic management guidelines that provide network management personnel with alternatives when emergencies occur. The forum also maintains contact directories for use in emergency situations.

Conclusions

While the information superhighway's development is expected to be arduous, a grand vision of its capabilities is beginning to emerge among policymakers, industry leaders, and public interest groups. Viewed as a global metanetwork that will seamlessly and reliably link millions of users through broadband terrestrial and satellite digital networks, it is hoped that the superhighway will allow users to routinely receive and transmit large volumes of digital information, and ensure equal access for service and network providers. Achieving the grand vision will depend largely on how successfully industry and government meet the key technical challenges of security and privacy, interoperability, and reliability.

Security and privacy of databases and users' communications is a critical issue. The superhighway will become an increasingly enticing target for intruders with the technical expertise and resources to cause damage. Given the complexity, size, and importance of the evolving superhighway, significant effort will be needed to define, develop, test, and implement security measures.

Interoperability among the thousands of networks, communications devices, and services that will comprise the superhighway is also essential, but will be difficult to achieve. The telecommunications industry is deploying, or plans to deploy, a host of technologies and services that are based on ill-defined, anticipatory, or competing standards. A coordinated approach will help reduce the risk of the superhighway being fragmented into thousands of poorly integrated networks providing a bewildering choice of incompatible services.

Because the proposed superhighway is intended to provide critical commercial and personal services, its end-to-end reliability requirements will be very high. The public and private sectors are already highly dependent on the existing telecommunications infrastructure and networks that will be the foundation of the superhighway. Outages on these networks have raised concerns about achieving reliability.

Government and industry are beginning to recognize these challenges. The administration's Information Infrastructure Task Force, working together with the private sector, has formed committees and working groups charged with addressing security and privacy, interoperability, and reliability issues. The challenge remains for the major public and private players to work together to resolve these issues. With effective cooperation, the promise of the information superhighway can be attained.

Information Infrastructure Task Force Is Addressing Selected Technical Issues

The administration formed the Information Infrastructure Task Force (IITF) to articulate and implement its vision for the information superhighway. The task force includes high-level representatives of federal agencies that play a major role in the development and application of information and telecommunications technologies. Working together with the private sector, the participating agencies plan to develop comprehensive technology, telecommunications, and information policies and promote applications that best meet the needs of both the agencies and the country. By helping build consensus on difficult policy issues, the IITF is planning to enable agencies to make and implement policy more quickly and effectively.

The Secretary of Commerce chairs the IITF, and much of the staff work and administrative support for the task force is being done by Commerce's National Telecommunications and Information Administration. The task force operates under the aegis of the White House Office of Science and Technology Policy and the National Economic Council. The administration has also established the United States Advisory Council on the National Information Infrastructure to facilitate private sector input to the IITF. The Secretary appointed 37 members to serve a two-year term on the advisory council. The council members represent the many different stakeholders in the information superhighway, including industry, labor, academic, public interest groups, and state and local governments.

The task force is undertaking a wide-ranging examination of all issues relevant to the development and growth of the information superhighway. The Administration's Agenda for Action, released September 15, 1993, identified nine specific principles and goals to guide government action:

- promoting private sector investment,
- extending the "universal service" concept to ensure that information resources are available to all at affordable prices,
- promoting technological innovation and new applications,
- promoting seamless and interactive operation,
- ensuring information security and network reliability,
- improving management of the radio frequency spectrum,
- protecting intellectual property rights,
- coordinating with other levels of government and with other nations, and
- providing access to government information and improving government procurement

To carry out its responsibilities, the IITF established three committees—Telecommunications Policy, Information Policy, and Applications and Technology. The Telecommunications Policy Committee is responsible for formulating a consistent administration position on key telecommunications issues. The committee has established the following four working groups:

- The universal service working group works to ensure that all Americans have access to and can enjoy the benefits of the information superhighway.
- The network reliability and vulnerability working group works to (1) ensure that the superhighway will provide protection for all users from catastrophic failure of the network, along with mechanisms for recovery from threats ranging from natural disasters to overt attacks; and (2) define and monitor national security and emergency preparedness requirements.
- The international telecommunications working group examines international telecommunications issues. This working group is subdivided into five subworking groups that are addressing:
  - the participation of foreign governments/foreign corporations in the superhighway and the use of the superhighway to open overseas markets,
  - the effects of current law on setting policy, and legislative efforts to change the law,
  - the federal government's controls of technology exports,
  - U.S. participation in international organizations and standards-setting bodies, and
  - international use of research networks.
- The legislative drafting task force is to formulate the administration's telecommunications legislative reform initiatives.

The Information Policy Committee has five working groups that are addressing critical information policy issues:

- The intellectual property rights working group is to develop proposals for protecting copyrights and other intellectual property rights in an electronic world.
- The privacy working group is to develop proposals to protect individual privacy.
- The government information working group is to focus on ways to promote dissemination of government data in electronic form.

- The Freedom of Information Act legislation working group is to define public access rights to government electronic records.
- The scientific and technical information group is to focus on ways to manage technical and scientific information.

The Committee on Applications and Technology coordinates the administration's efforts to develop, demonstrate, and promote applications of information technology in manufacturing, education, health care, government services, libraries, environmental monitoring, electronic commerce, and other applications. It has three working groups:

- The government information technology services working group coordinates efforts to improve the application of information technology by federal agencies.
- The technology policy working group addresses cross-cutting technology issues related to interoperability and scalability of new telecommunications and information services.
- The health information and applications working group coordinates efforts that affect use of the superhighway for health care.

The IITF has also established the NII Security Issues Forum to coordinate security efforts across the committees and working groups of the IITF.

Description of Existing Network Technologies

The following provides a brief overview of the three major types of communication networks that comprise the existing communication infrastructure—the wire-based voice and data telephone networks; the cable-based video networks; and the wireless, voice, data, and video networks.

The Telephone Networks

The telephone system is the world's largest switched distributed network providing point-to-point voice, fax, data, and videoconferencing services to hundreds of millions of subscribers. It is also, at first glance, the primary foundation for the information superhighway. It is ubiquitous, highly interoperable, and reliable. It is capable of handling millions of simultaneous calls, and it provides accurate usage tracking and billing. In the U.S., voice, data, and videoconferencing services are provided by the local exchange carriers (local telephone companies) serving the local access and transport areas, and by the interexchange carriers (long distance carriers) providing long distance and international dialing services through their long distance networks.[1] Although the industry is rapidly introducing advanced digital communication technologies, the telephone network continues to be dependent on analog transmission.[2]

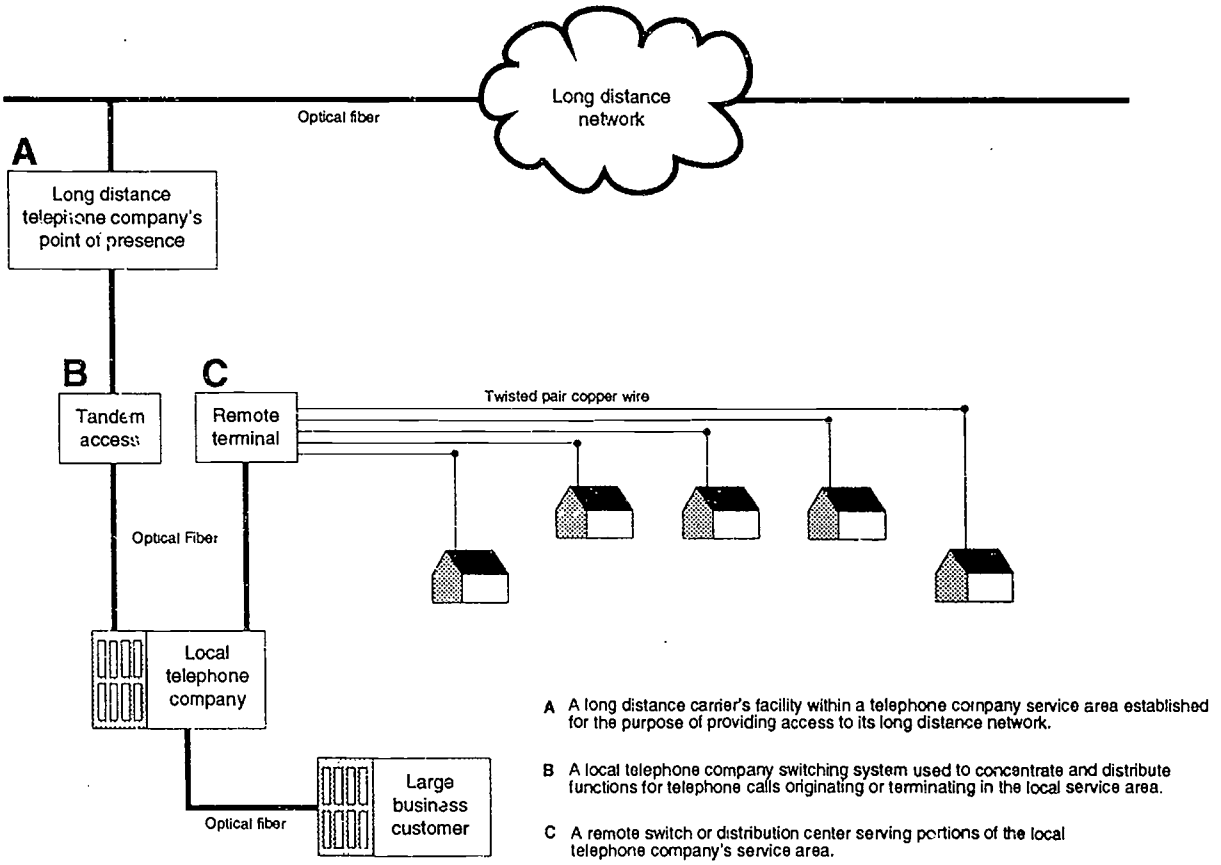
Much of today's telephone service is based on two analog-oriented transmission technologies—the analog voice frequency (VF) systems and the digital T-carrier system. The VF system supports voice transmission over a pair of copper wires—also known as the local loop—connecting millions of residential and business subscribers with the local telephone company's central offices. The T-carrier system plays a major role in the first step in the transition from analog to digital capabilities. One of the fastest growing segments of services offered by the local telephone companies and the long distance carriers, the system can provide transmission speeds up to 274.176 Mbps. The basic building block of the T-carrier technology is a single VF voice channel digitized into a 64 Kbps data stream; a T-1 line carries 24 digitized voice channels, an aggregate of 1.544 Mbps. The T-carrier digital hierarchy allows T-1 lines to be combined to provide transmission rates of up to 274.176 Mbps.

[1]The local telephone companies, created in the wake of the breakup of AT&T, include 22 Bell Operating Companies organized into seven regional Bell holding companies—Pacific Telesis, US West, Ameritech, Southwestern Bell, BellSouth, Bell Atlantic, and NYNEX. Many local area and transport areas are also served by independent telephone companies. The major long distance carriers include AT&T, MCI, U.S. Sprint, Advanced Telecommunications Corporation, and Wiltel.

[2]During the 1980s, the telephone service providers replaced most of their older electromechanical switches with analog or digital computer-driven switches.

The telephone network's capabilities are unevenly distributed. Most of the high-capacity fiber optic lines capable of carrying interactive video and other bandwidth-intensive applications are either part of the long distance or the local telephone area interoffice networks, or are used by the telephone companies to provide private voice, data, and videoconferencing services to business, government, and institutions. The bandwidth available to residential subscribers is effectively constrained by the limited transmission capacity of the copper wire linking the local telephone company's central office with the subscriber's instrument, and the lack of subscriber's equipment capable of providing broadband services. Similarly, although the local telephone companies generally use digital switches to route telephone calls, in most cases the calls are converted back to analog format for transmission to individual subscribers. The basic architecture of a typical telephone network is shown in figure II.1.

Figure II.1: A Typical Local Telephone Network



Source: Adapted from the "Hybridizing the Local Loop," Craig J. Burnet, IEEE Spectrum, June 1994.

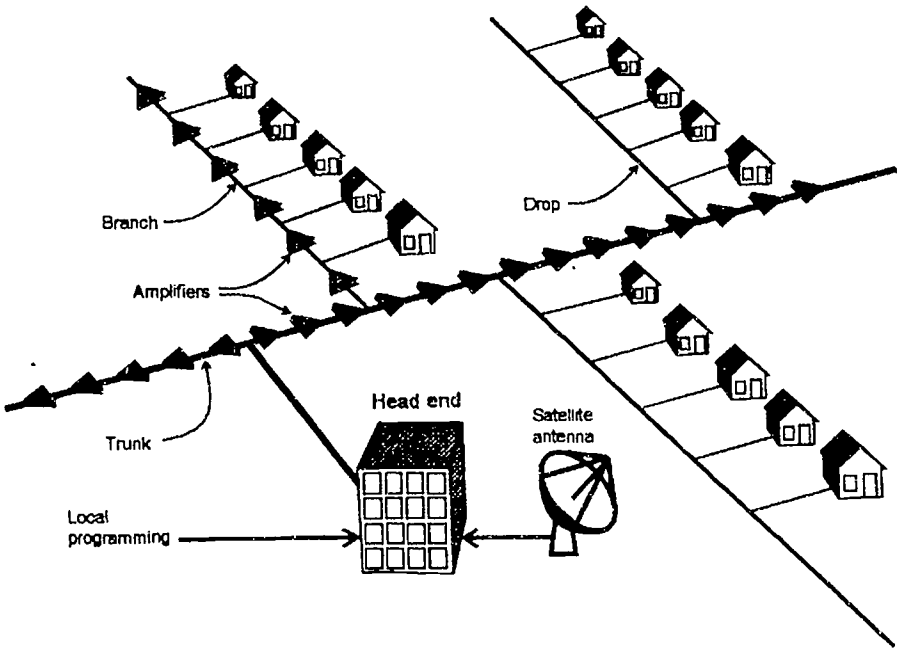
Cable Television Network

The nation's cable television network links thousands of cable systems with millions of subscribers via broadband coaxial cable.[3] This web of coaxial cables is, in many respects, a counterpart of the local loop linking telephone subscribers with the local telephone companies. However, there are considerable differences between the transmission technologies and network architectures deployed in the telephone and the cable systems.

[3]During the last decade, the cable television industry experienced considerable growth, from 4,225 systems serving 17.7 million subscribers in 1980, to 11,075 cable systems serving over 57 million subscribers. Today, cable service—or ready access to the service provider's coaxial cable—is available to over 96 percent of the nation's homes.

The telephone system is based on a switched, distributed network architecture, and uses standard switching and transmission protocols capable of supporting global, narrowband, two-way, point-to-point communications. The cable systems, on the other hand, are based on a tree-and-branch network architecture and proprietary transmission protocols designed to support one-way broadband analog transmission with little or no provision for "upstream" communications. The basic architecture of a typical cable system is shown in figure II.2.

Figure II.2: A Typical Cable System Architecture



Wireless Networks

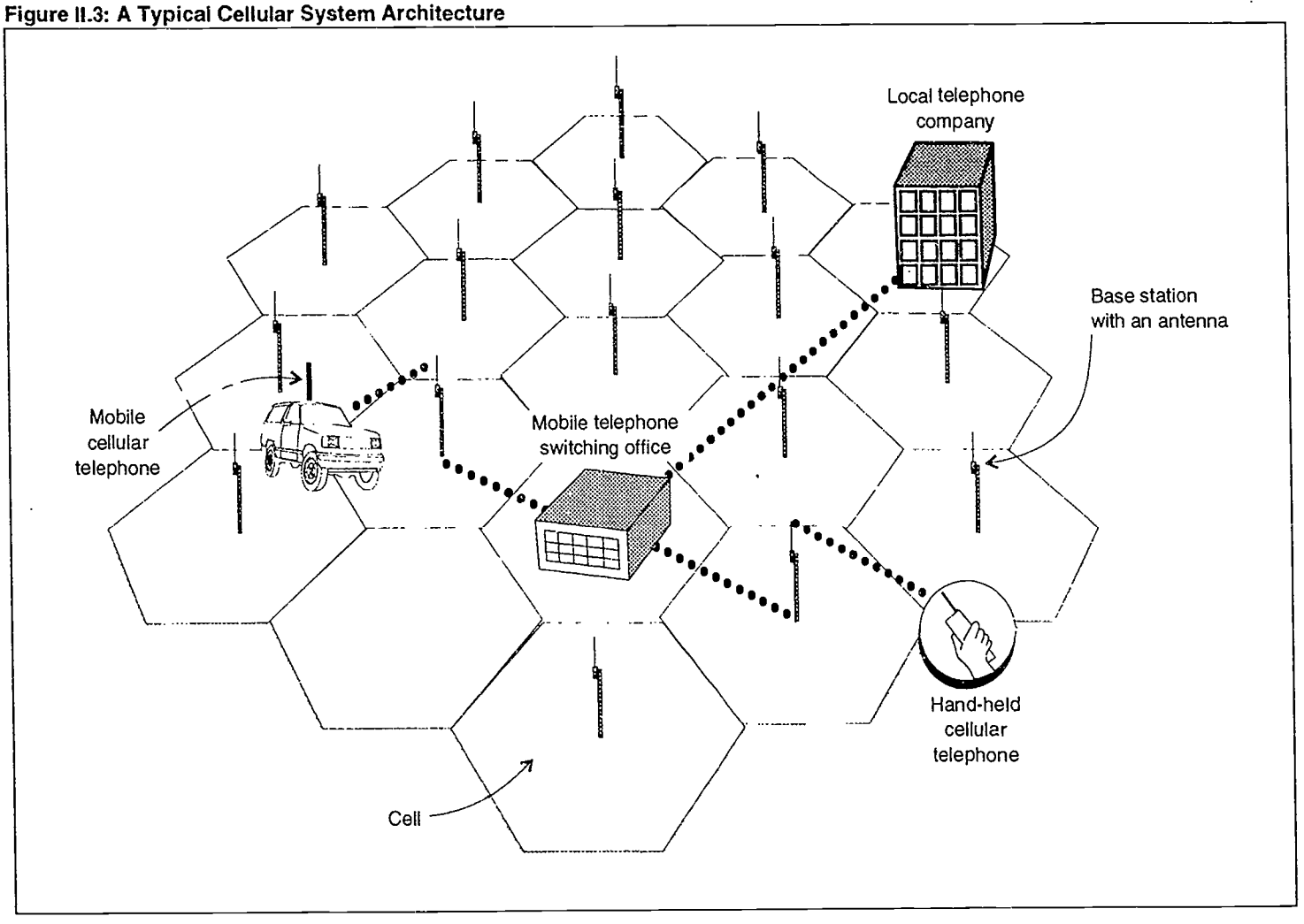
Wireless networks are an important element of the communications infrastructure. These systems—including cellular and space-based systems and networks—are providing users with an unprecedented degree of mobility and flexibility. The cellular and satellite networks have advantages over terrestrial networks because they are potentially accessible from any point on the globe without the cost of installing wire or a cable. The current analog cellular services were developed in the early

1970s to alleviate growing radio frequency spectrum congestion and to overcome the limited capacity of the early mobile radio systems. In the cellular systems, this is accomplished by dividing a large geographic service area into discrete regions—or cells—each of which is served by a low-power base station transmitting to and receiving from mobile telephones within its area. The use of low-powered transmitters operating on short-wavelengths allows the cellular systems to efficiently exploit the available radio spectrum by "reusing" the assigned radio frequencies throughout the service area.[4] However, the analog cellular systems have not fulfilled their early promise. In many large metropolitan markets, the systems are saturated and will be slowly supplemented, and eventually replaced, with digital systems.[5] The architecture of a typical cellular system is shown in figure II.3.

[4]In the U.S. and in several other countries, the analog cellular systems are based on the Advanced Mobile Phone Services standard. This standard provides 416 voice channels and employs a seven-cell frequency reuse pattern.

[5]The FCC requires that any new digital cellular system be fully compatible with the current analog system. The new hand-held mobile units will be capable of either analog or digital operation.

Figure II.3: A Typical Cellular System Architecture



Satellite networks have advantages over terrestrial networks because they are accessible from any spot on the globe; can provide broadband digital services, including voice, data, and video, to many points without the cost of acquiring right-of-way and cable installation; and can add receiving and transmitting sites without significant additional costs. Commercially available since 1965, communications satellites are a critical part of the global communications infrastructure. Today, there are about 150 communications satellites in geosynchronous orbit (GEO) providing a wide

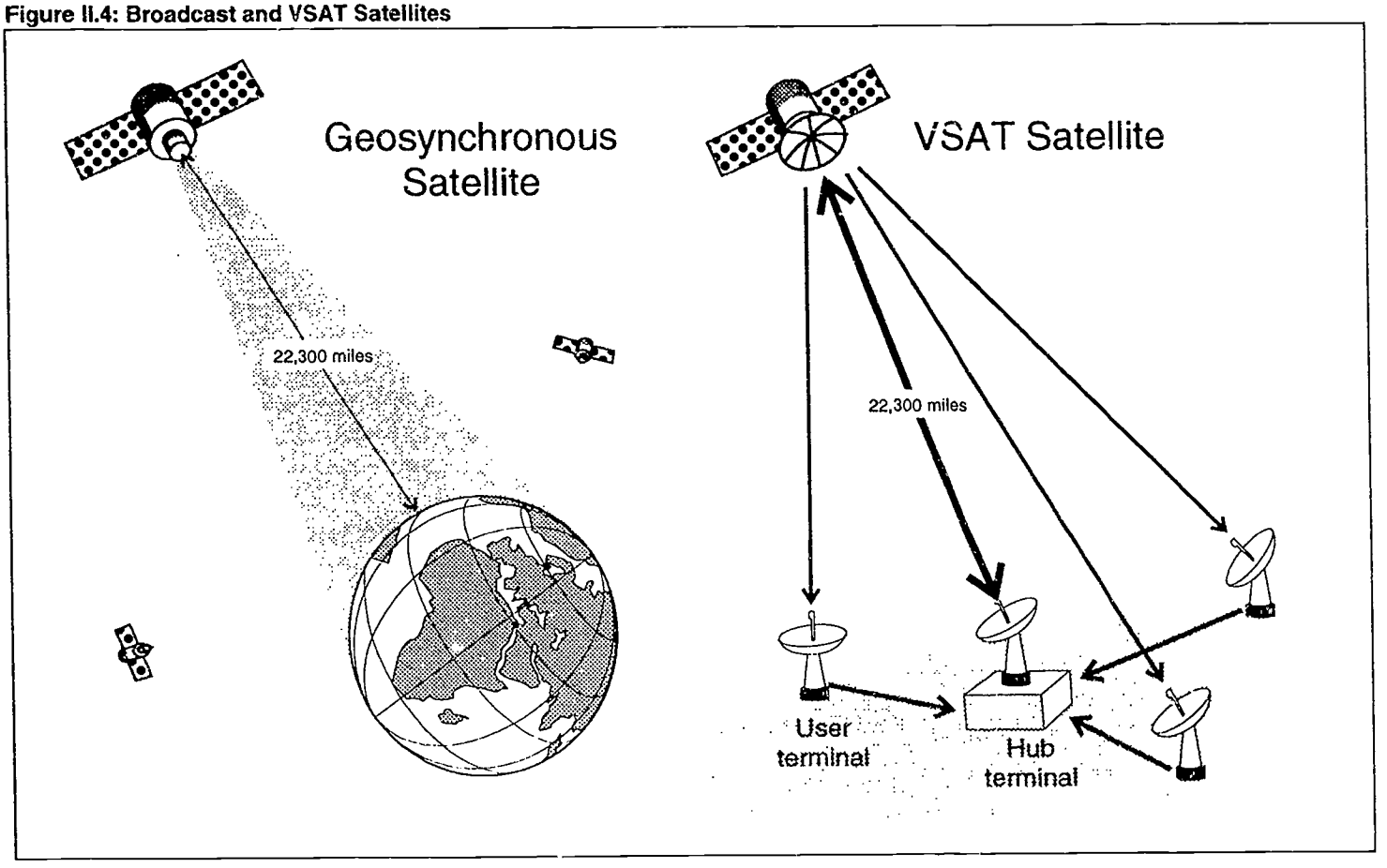
range of services, including broadcast video and overseas telephone links.[6]

In general, GEO satellites are designed to broadcast a wide beam to ensure the coverage of a large geographic area. Although such a large broadcast "footprint" allows only three GEO satellites to provide nearly global coverage, the network's receiving stations require large antennas to capture the relatively weak signal.

In the 1980s, industry introduced a new class of satellites using a narrow beam to focus the transmitted energy on a small geographic areas. Known as very small aperture terminal (VSAT) satellites, the new breed of satellites use small ground antennas to provide low data rate point-to-point network services. VSAT networks are being increasingly used by large corporations to link hundreds of motel/hotel or retail sites. Figure II.4 shows a typical GEO broadcast and VSAT satellite system based on a hub and spoke relay configuration. Because this configuration does not allow direct terminal-satellite-terminal relays, all communications must be routed through the hub terminal.

[6]GEO satellites are placed in a high circular orbit 22,300 miles above the equator. Because GEO satellites rotate with the Earth, they appear to be stationary.

Figure II.4: Broadcast and VSAT Satellites



Description of Advanced Technologies

The communications industry is beginning to introduce several new and innovative technologies that will allow the delivery of many of the advanced services and capabilities of the information superhighway. These technologies include

- narrowband ISDN,
- advanced signaling and intelligent networks,
- B-ISDN,
- personal communications networks, and
- broadband in the local loop.

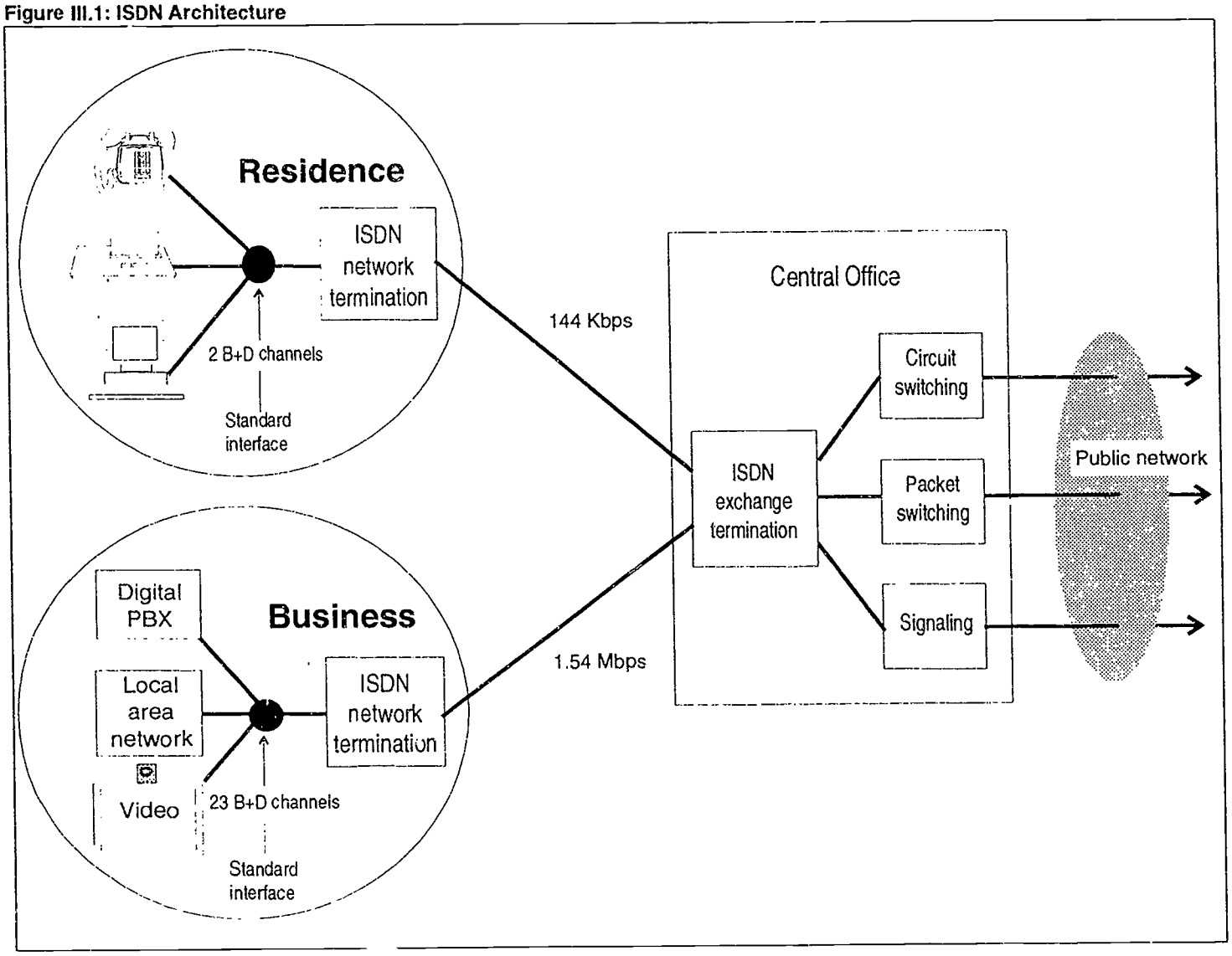
The Narrowband ISDN

One of the emerging technologies that will be key to the future superhighway is the narrowband ISDN. Deployment of this technology is the first step in the conversion from the existing networks to a fully digital network. ISDN is an end-to-end digital network that is evolving from the existing telephone network. It is already providing some users with direct access to digital transmissions—at speeds ranging from 144,000 bits per second (144 Kbps) to 1.544 Mbps—capable of handling many different forms and types of information, including conventional analog voice, digital voice, and packet data.

Because of poorly defined standards, the early implementations of ISDN were plagued with interoperability problems. In an effort to effectively manage the integration of the ISDN technology with the public switched networks, the industry has adopted a set of standards known as the National ISDN. National ISDN will include advance signaling capabilities, as well as a wide range of digital services.

Telecommuting or work-at-home is one area where the benefits of ISDN service can be readily identified. Currently, an employee working at home may have to install additional telephone lines to handle computer and fax communications. Using ISDN, the telecommuter can communicate—over a single line—with the employer's local area network, while simultaneously carrying on a telephone conversation with a colleague and receiving a fax from the employer's office. Similarly, as shown in figure III.1, a large business or institutional ISDN customer can use ISDN to consolidate voice, data, and videoconferencing services.

Figure III.1: ISDN Architecture



Source: Adapted from A Guide to New Technologies and Services, Bellcore, 1993; figure 4-1, pp. 4-7.

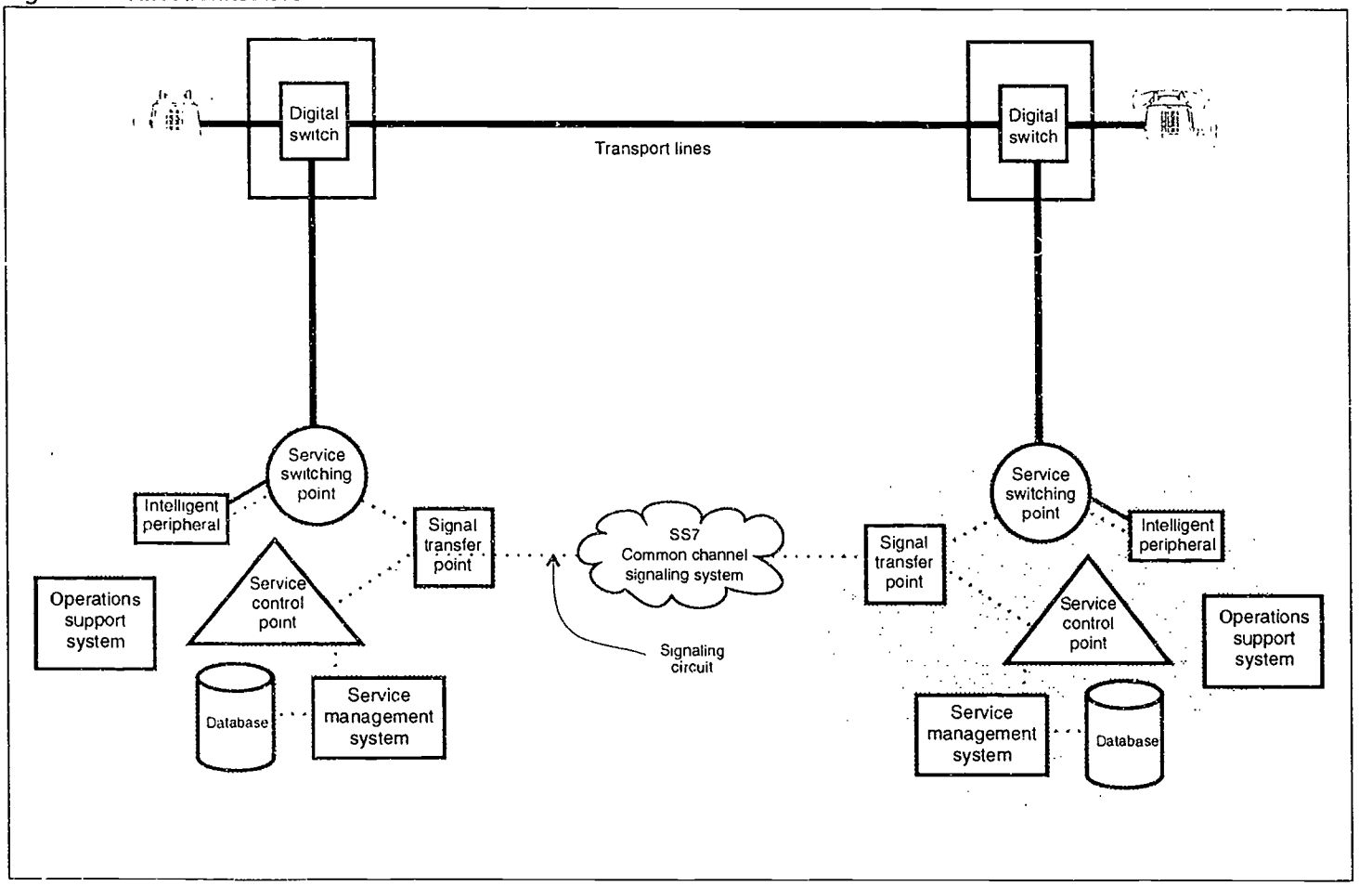
Advanced Signaling and Intelligent Networks

In order to offer new services and advanced capabilities, such as 800 number and ISDN services, the telephone industry is deploying common channel signaling networks. These networks are based on the Signaling System 7 (SS7) protocol. An SS7 network is a packet-switched communications network that transports call control and signaling

messages on a dedicated high-speed data network separate from the voice or data communications networks. The SS7 provides capabilities critical to the development of advanced intelligent networks (AIN). A programmable AIN network provides the capability for network switches to interrogate remote processors, databases, and mobile communications devices. The network intelligence resides in on-line, real-time databases, rather than in every switch, and is accessed through the SS7 signaling system. Such intelligent networks allow greater customer control, provide the tools for the creation of virtual private networks, increase competition by allowing competing carriers to use the AIN capabilities to offer custom services, and provide the mechanisms for alternative call destination routing required by the emerging personal communications services (PCS).[1] Figure III.2 shows a simplified view of an AIN architecture.

[1]PCS is a new type of service designed to support hand-held personal voice and data communications terminals. Mobile PCS users are expected to be able to receive services such as high-quality voice, data, facsimile, and video at any terminal anywhere the user has directed his or her calls.

Figure III.2: AIN Architecture



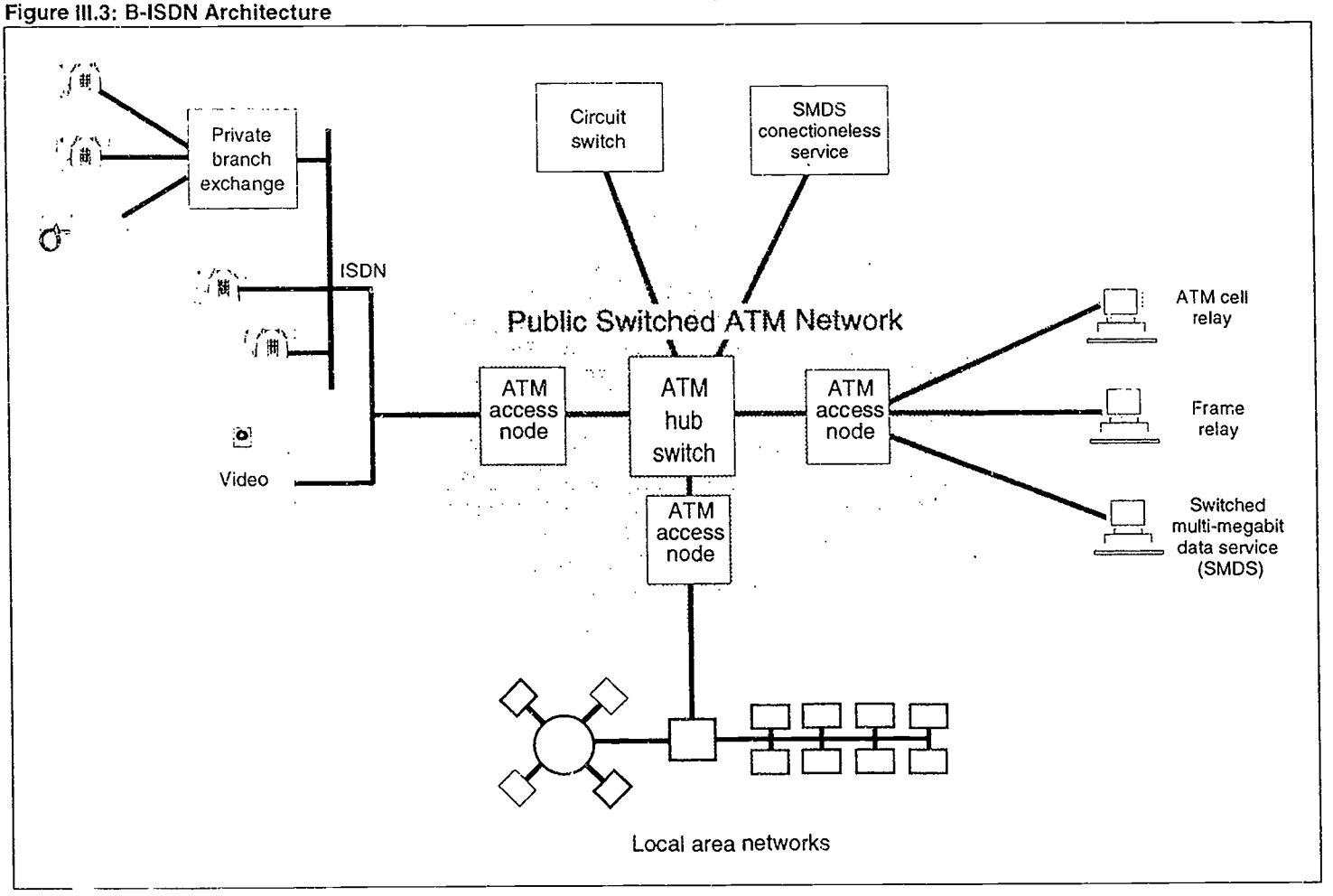
Source: Adapted from A Guide to New Technologies and Services, Bellcore, 1993; figure 1-1, pp. 1-5

B-ISDN Technologies

The B-ISDN technology is a dramatic departure both from the existing digital infrastructure and the narrowband ISDN concept. Because it will provide transmission rates up to 2,488 Mbps, B-ISDN will not be able to use the existing digital infrastructure, but will largely rely on the Asynchronous Transfer Mode (ATM)/Synchronous Optical Network (SONET) optical fiber networks. SONET, an international standard for optical carrier networks, provides a variety of transmission rates in multiples of 51.84 Mbps, with currently deployed optical circuits operating between 156 to 622 Mbps, and with future circuits expected to operate at up to 2,488 Mbps. SONET will support B-ISDN using the ATM standard. While SONET is one

of the transmission technologies that provides the high-speed transmission system required by the information superhighway, ATM will allow users to transmit a rich mix of data during a single transmission session. Figure III.3 provides an overview of the B-ISDN architecture.

Figure III.3: B-ISDN Architecture



Source. Adapted from A Guide to New Technologies and Services, Bellcore, 1993; figure 2-6, pp 2-11

Much remains to be done to develop a global integrated B-ISDN network. Although the local and long distance telephone companies are beginning

to deploy ATM/SONET networks, ATM standards are continuing to evolve. For example, several standards, including service quality, transmission routing, and encryption standards, have not yet been defined. The Advanced Research Projects Agency and the National Science Foundation, in coordination with industry, are actively pursuing investigations focused on the development of ATM standards and network management tools. These two agencies established five gigabit network research testbeds focused on ATM network technology, alternative network architectures, and applications. In addition, the Advanced Research Projects Agency is evaluating the best commercial prototypes of ATM/SONET technology and related applications, including ATM satellite connections and the encryption of gigabit data streams.

Personal Communications Networks

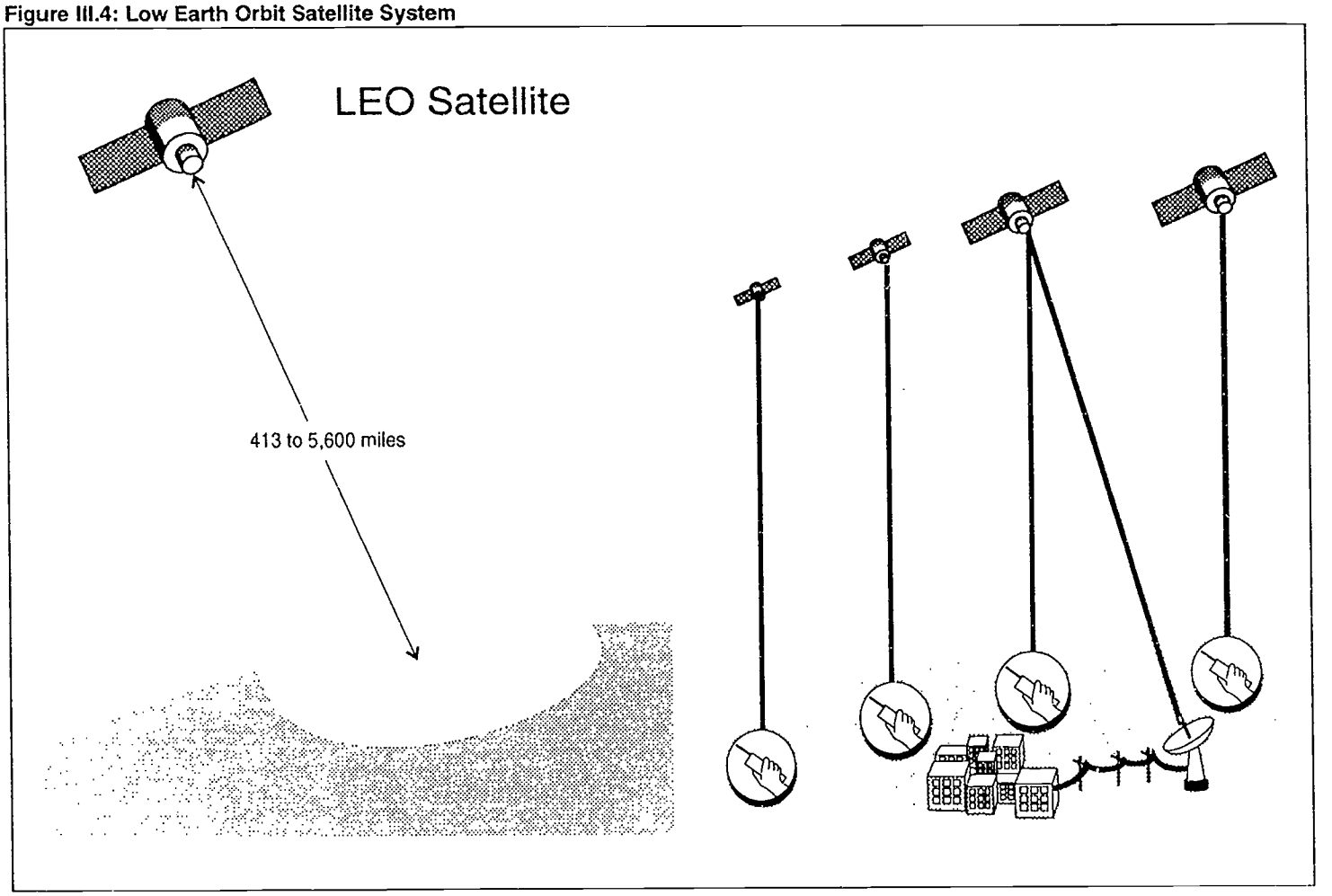
Some observers believe that we are moving toward a ubiquitous, tetherless global metanetwork composed of cellular and satellite communications systems supplemented by wire-based ground networks. Personal communications networks (PCN) and the related personal communications services (PCS) are expected to be an important part of this tetherless metanetwork. PCNs are based on a concept of tetherless digital communications systems providing mobile users with worldwide connectivity. Unlike the station-to-station connectivity provided by the existing telephone systems, PCNs will provide person-to-person access using a national—and potentially worldwide—personal numbering concept.

Digital wireless communications, cellular systems, and the AIN capabilities of the evolving B-ISDN networks are expected to play a crucial role in the development of PCNs. Initially, PCNs will include a diverse mix of analog and digital technologies and services—cellular systems, mobile satellite systems, paging, and local area networks—based on radio access technology and interfaced with the wire-based public networks. It is expected that a full-scale PCN will deploy a combination of technologies, mostly because the terrestrial wire and cellular networks will not provide worldwide connectivity, particularly to users in remote areas. To achieve this objective, the terrestrial cellular systems may be complemented by space-based cellular type services.

There are two basic approaches to space-based PCNs. One uses satellites in high geosynchronous earth orbit (GEO), while the other relies on a constellation of low-earth orbit (LEO) satellites. The GEO systems, being in higher orbit, require more power at both the transmitter and the receiver

than the LEOs, but provide more earth coverage with fewer spacecraft. On the other hand, LEO systems, while cheaper on a unit-basis, require far more satellites to provide earth coverage. In general, most of the recently proposed space-based PCNs are focused on LEO systems, including Motorola's Iridium system (77 satellites), TRW's Odyssey system (12 satellites), Leosat's system (18 satellites), and the recently announced network of 840 satellites proposed by the Teledesic Corp. Figure III.4 show a typical LEO satellite network.

Figure III.4: Low Earth Orbit Satellite System



Broadband in the Local Loop

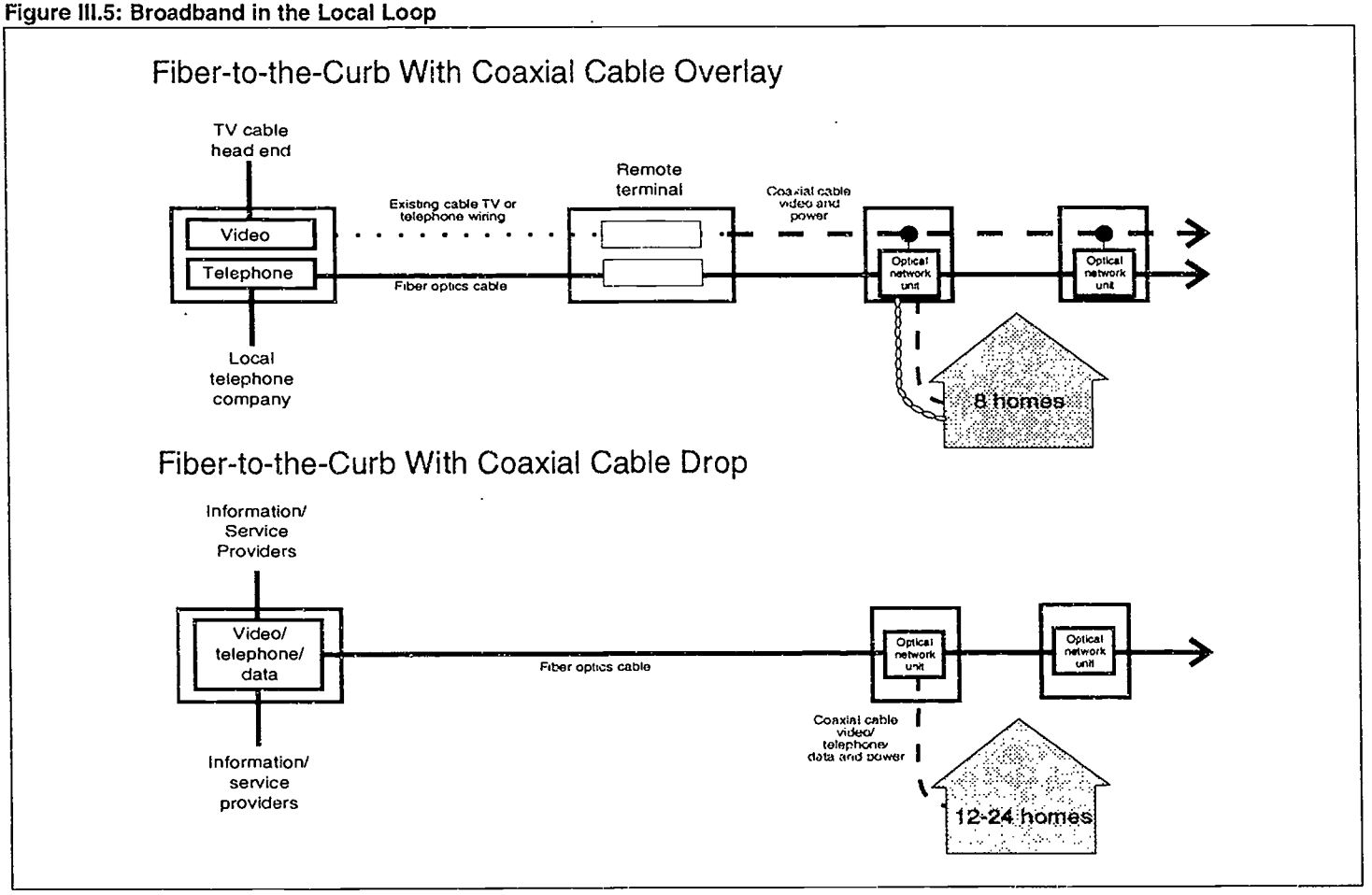
While industry is upgrading the transport layer and laying thousands of miles of optical fiber, the on-ramps that will link the high-speed portions of

the national information infrastructure with homes, business, and institutions continue to form a bottleneck to high-speed information flow. In the near term, the primary challenge will be to provide broadband digital services over the existing plant—the hundreds of thousands of miles of copper wire and coaxial cable—although ultimately it may be preferable to provide fiber optics to each residence. The replacement cost for this "last mile" of the superhighway—linking the broadband backbone with residences, business, and institutions—continues to be high, not only because there is so much copper wire and coaxial cable to be replaced, but also because of the need for special equipment to process the optical signal on the customer's premises.

The telephone and cable companies are adopting a mix of technologies and strategies to cope with the bottleneck in the local loop—the portion of the telephone communication circuit connecting individual subscribers with the telephone company's central office. For the telephone companies, the most promising approaches are the asymmetrical digital subscriber line and the fiber-to-the-curb architectures. The asymmetrical digital subscriber line allows telephone companies to use a single copper wire to simultaneously transmit video and telephone signals by increasing the transmission speed from 64 Kbps to 1.5 Mbps while providing an upstream channel between 16 to 384 Kbps. The fiber-to-the-curb architecture provides high-capacity switched digital network services to optical network units serving multiple residences. Optical network units house the necessary equipment to convert the optical signals to electrical impulses and distribute them to individual homes over a copper wire or coaxial cable.

Most of the newer or rebuilt cable systems also use a hybrid fiber optics/coaxial cable architecture, commonly known as fiber trunk feeder. This hybrid fiber optics/coaxial cable architecture is capable of supporting all digital, fully switched ATM/SONET services. Figure III.5 highlights two fiber-to-the-curb architectures that may be used by the telephone and cable industries to deliver broadband services to subscribers.

Figure III.5: Broadband in the Local Loop



Ensuring the Portability of Telephone Numbers Poses a Challenge

The ability of the public networks to efficiently route and deliver electronic communications is heavily dependent on the efficient allocation and use of a limited resource—the pool of available ten-digit telephone numbers. In recent years, the proliferation of telecommunications services and providers has placed increasing demands on this resource. More importantly, new requirements, such as demands for (1) personal mobility, whereby communications services are provided to individuals, rather than to fixed geographic locations (for example geographic mobility), and (2) number portability, whereby customers are able to change service features and providers quickly without needing to change their telephone number, will significantly alter the way we manage the numbering resources.

The first demand—the provision of services to individuals rather than fixed geographic locations—will be largely satisfied by emerging PCSs. PCSs will exploit the capabilities of AIN and nongeographic telephone numbers to provide wireless or land-line based services to "roaming" individuals. The second demand—the assignment of a permanent "personal" telephone number to individuals—will require the development of national or regional databases containing the personal numbers and customer service profiles. Although there are no insurmountable technical barriers to number portability, industry's experience with the development of full portability for the 800 number services indicates that it will be a lengthy and arduous process.[1]

The North American Numbering Plan Guides the Management of Numbering Resources

The basic telephone numbering scheme, known as the North American Numbering Plan (NANP), was developed the Bell System. In 1984, following the AT&T divestiture, the numbering plan functions performed by AT&T were transferred to Bell Communications Research (Bellcore). Since that time, Bellcore has served as the NANP administrator. Under NANP, each telephone within the World Zone 1[2] can be reached by dialing a unique ten-digit number generally composed of three parts—a three-digit geographic area code, a three-digit secondary code, and a four-digit "station" or "line" code.

[1]It took almost 7 years for industry to implement full portability for 800 service.

[2]The World Zone 1 includes the United States, Canada, Bermuda, and most of the Caribbean. It provides a uniform dialing scheme applicable in 18 countries, and serves more than a thousand local exchange carriers, several hundred long distance carriers, and over one hundred million customers. International calls to countries not included in the NANP require the dialing of country codes; thus telephone numbers can differ in length from country to country.

However, under the current format, there are only 160 possible area codes. These represent the number of combinations available when the first digit cannot be zero or one, and the second digit is always zero or one. Sixteen of the codes have a unique format: eight have a double "0" ("N00" codes) and eight have a double "1" ("N11" codes). The N00 codes are called Service Access Codes (SAC).[3] The most widely recognized SACs are the 800 and 900 codes. The N11 codes are known as "service codes" and are set aside for special functions, the most widely used being the 911 emergency code. All of the remaining 144 codes are assigned and it has been long expected that the present stock of codes would be exhausted sometime in the 1990s.

A numbering relief plan, scheduled to be implemented in January 1995, will expand the number of potential codes from 160 to 800. This expansion will be accomplished by allowing the second digit of the area code to include the digits "2" through "9" in addition to "1" and "0". For example, area code 334 is scheduled to be placed in service in northern Alabama on January 15, 1995. The addition of 640 new codes will not only significantly increase the numbering resource, but may also provide additional codes for nongeographic assignment such as the "personal" numbers needed for PCS users. Because the new codes will not be available until 1995, carriers anxious to offer PCS asked Bellcore for the assignment of one of the four nongeographic codes (500 SAC) for PCS. The carriers plan to offer PCS that includes personal mobility, terminal mobility, and service profile services, but not, at least initially, number portability. In essence, PCS users would have to be issued a new telephone number every time they changed a PCS provider.

Portability Issues Remain Unresolved

In June 1993, Bellcore informed the FCC that it had decided, absent instructions to the contrary, to proceed with the assignment of 500 SAC for PCS service to carriers that had expressed an urgent need for these assignments. In response to Bellcore's notification, the FCC requested public comments on the proposed assignment of the 500 SAC for PCS, and directed Bellcore to delay the assignments until it had a chance to consider the comments. At the same time, FCC asked Bellcore to submit, within 30 days, a detailed proposal for achieving 500 number portability. In response, Bellcore noted that there were many ways to achieve number portability, but did not offer a concrete proposal. An industry workgroup is addressing the issue of PCS number portability. Bellcore began assigining

[3]Three SAC's (700, 800, and 900) are currently in use through World Zone 1; one (600) is assigned to the Canadian government, while the 500 SAC has been assigned for roaming PCS.

numbering resources within the 500 SAC for roaming services after the FCC considered the comments on the issue and gave its approval in May 1994. Bellcore also notified the FCC that because of the many changes in the telecommunications environment which have resulted in increased controversy regarding numbering, Bellcore and its owners believed that it was time to relinquish Bellcore's voluntary administration of the NANP.

The FCC has yet to take final action in finding a replacement for Bellcore or to act on the 500 SAC portability issues. According to the United States Telephone Association, it appears unlikely that the initial PCS services will provide number portability. Full national number portability may not be available for years, given that the design and deployment of a database architecture for the 500 SAC will take considerable time.

Major Contributors to This Report

Accounting and Information Management Division, Washington D.C.	Rona B. Stillman, Chief Scientist for Computers and Communications Ronald W. Beers, Assistant Director Mirko J. Dolak, Evaluator-in-Charge John P. Rehberger, Staff Evaluator Shane D. Hartzler, Reports Analyst Susan B. Willson, Secretary
Office of General Counsel	John A. Carter, Senior Attorney
Resources, Community, and Economic Development Division	Paul J. O'Neill, Assistant Director Edmond E. Menoche, Senior Evaluator
Boston Regional Office	Bruce Holmes, Assistant Director

Glossary

The definitions in this glossary are drawn from several sources, including the Computer Dictionary: The Comprehensive Standards for Business, School, Library, and Home, Microsoft Press, 1991, Washington, D.C.; The McGraw-Hill Telecommunications Factbook, McGraw-Hill, New York, 1993; The New IEEE Standard Dictionary of Electrical and Electronic Terms, The Institute of Electrical and Electronic Engineers, New York, 1993; and the Auerbach Data Communication Management, Auerbach Publishers, Pennsauken, New Jersey, 1994.

Address	A sequence of bits or characters that identifies the destination and the source of a transmission.
Advanced Intelligent Network	An evolving architecture that allows rapid creation and modification of telecommunications services.
Agile Manufacturing	An approach to industrial production that allows a manufacturer to rapidly respond to market demand by reducing the time it takes to design and manufacture a product. Also known as rapid response or demand activated manufacturing.
Amplitude	A relative magnitude of a signal.
Analog	A term applied to any device, usually electronic, that represents values by a continuously variable physical property, such as voltage in an electronic circuit. An analog device can represent an infinite number of values within the range the device can handle. In contrast, digital representation maps values onto discrete numbers, limiting the possible range of values to the resolution of the digital device.
Analog Signal	A continuous electrical signal whose amplitude varies in direct correlation with the original input.
Architecture	A general term referring to the structure of all or part of a computer system. The term also covers the design of system software, such as the operating system, as well as refers to the combination of hardware and basic software that links the machines on a computer network. Computer architecture refers to an entire structure and to the details needed to make

	it functional. Thus, computer architecture covers computer systems, chips, circuits, and system programs, but typically does not cover applications, which are required to perform a task but not to make the system run.
Asynchronous Operation	Generally, an operation that proceeds independently of any timing mechanism, such as a clock. In communications, for example, two modems communicating asynchronously rely upon each one sending the other start and stop signals in order to pace the exchange of information.
Asynchronous Transfer Mode	A fast-packet technology that was developed for use in area networks using fixed-length cells. Current ATM standards allow it to scale from speeds of 155 Mbps to 622 Mbps over fiber networks. ATM appears to be the best alternative for multimedia applications where data are mixed with voice, images, or full-motion video.
Bandwidth	In communications, the difference between the highest and lowest frequencies in a given range. For example, a telephone accommodates a bandwidth of 3000 hertz (Hz), the difference between the lowest (300 Hz) and highest (3300 Hz) frequencies it can carry. In computer networks, greater bandwidth indicates faster data-transfer capabilities.
Basic Rate Interface	Transmission rates for the integrated service digital network. Basic rate interface consists of two 64 Kbps channels and one 16 Kbps channel packet-switched data channel used for signaling and packet data transmission functions.
Bit	Short for "binary digit"; either 1 or 0 in the binary number system. In processing and storage, a bit is the smallest unit of information handled by a computer and is represented physically by an element such as a single pulse sent through a circuit or a small spot on a magnetic disk capable of storing either a 1 or a 0. Considered singly, bits convey little information a human would consider meaningful. In groups of eight, however, bits become the familiar bytes used to represent all types of information, including the letters of the alphabet and the digits.

Broadband Network	A type of local area network on which transmissions travel as radio-frequency signals over separate inbound and outbound channels. Stations on a broadband network are connected by coaxial or fiber-optic cable. The cable itself can be made to carry data, voice, and video simultaneously over multiple transmission channels. This complex transmission is accomplished by the technique called frequency-division multiplexing, in which individual channels are separated by frequency and buffered from one another by guard bands of frequencies that are not used for transmission. A broadband network is capable of high-speed operation (20 megabits or more), but it is more expensive than a baseband network and can be difficult to install. Such a network is based on the same technology as is used by cable television. Broadband transmission is sometimes called wideband transmission.
Capstone Chip	A data security chip. The Capstone chip, also known as MYK-80, incorporates NSA's Skipjack, key exchange algorithms, and the NIST digital signature and secure hash algorithms.
Cell	In celluiar systems, the smallest geographic area defined for mobile communications systems.
Cellular Systems	Mobile telephony systems employing hexagonal geographic areas, or cells, with group frequencies allocated to each cell. Typically, seven cells make a block, and no adjacent cell uses the same set of frequencies.
Ciphertext	The encrypted form of a plaintext message or data.
Circuit Switching	A method of opening communications lines, as through the telephone system, creating a physical link between the initiating and receiving parties. In circuit switching, the connection is made at a switching center, which physically connects the two parties and maintains an open line between them for as long as needed. Circuit switching is typically used in modem communications on the dial-up telephone network, and it is also used on a smaller scale in privately maintained communications networks.
Clipper Chip	A microcircuit that contains a classified secret-key encryption algorithm known as Skipjack. The Clipper chip family, manufactured by Mykotronx,

	Inc., includes three prototypes chips—the MYK-78E, MYK-78T, and MYK-77. MYK-78E and MYK-78T are designed for wirebased digital telephony. MYK-77 is designed for use in digital radios operating at low data rates. Also see Capstone Chip.
Coaxial Cable	Often referred to as coax or coax cable. A cable that consists of two conductors, a center wire inside a cylindrical shield that is grounded. The shield is typically made of braided wire and is insulated from the center wire. The shield minimizes electrical and radio-frequency interference; signals in a coaxial cable do not affect nearby components, and potential interference from these components does not affect the signal carried on the cable.
Code Division Multiple Access	A cellular digital standard that deploys frequency hopping—rapid change of frequency—with the carrier frequency continually shifted through a wideband channel.
Common Channel Signaling	A method of carrying signaling and supervisory information between telephone central offices in a separate, dedicated channel.
Communications Protocol	A set of rules or standards designed to enable computers to connect with one another and to exchange information with as little error as possible. The word "protocol" is used, sometimes confusingly, in reference to a multitude of standards affecting different aspects of communication. Some standards affect hardware connections, while other standards govern data transmission. Still other protocols govern file transfer, and others define the methods by which messages are passed around the stations on a local area network. Taken as a whole, these various and sometimes conflicting protocols represent attempts to facilitate communication among computers of different makes and models.
Computer Network	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area. Small or large, a computer network exists to provide

	computer users with the means of communicating and transferring information electronically. Some types of communication are simple user-to-user messages; others, of the type known as distributed processes, can involve several computers and the sharing of workloads or cooperative efforts in performing a task.
Cryptanalysis	The process of converting encrypted messages into plaintext without knowledge of the key employed in the encryption algorithm.
Cryptography	The transformation of ordinary text—or plaintext—and other data into coded form by encryption and the transformation of the coded text or data back to plaintext or data by decryption.
Cryptographic Algorithm	A mathematical procedure used for such purposes as encrypting and decrypting messages and signing documents digitally.
Cryptographic System	The hardware, software, documents, and associated techniques and processes that together provide a means of encryption.
Data Encryption Standard	A NIST Federal Information Processing Standard and a commonly used secret-key cryptographic algorithm for encrypting and decrypting data.
Digital	Related to digits or the way they are represented. In computing, digital is virtually synonymous with binary because the computers familiar to most people process information coded as combinations of binary digits, or bits—zeros and ones. One bit can represent at most two values—0 or 1. Two bits can represent up to 4 different values—00, 01, 11, and 10. Eight bits can represent 256 values—00000000, 00000001, 00000011, and so on.
Digital Signature	A cryptographic method, provided by public-key cryptography, used by a message's recipient or any third party to verify the identity of the message's sender and the integrity of the message. A sender creates a digital signature or a message by transforming the message with his or her private key. A recipient, using the sender's public key, verifies the digital

	signature by applying a corresponding transformation to the message and the signature.
Digital Signature Standard	A NIST Federal Information Processing Standard that supports digital signature.
Electronic Signature	See digital signature.
Encryption	The transformation of data into a form readable only by using the appropriate key, held only by authorized parties. The key rearranges the data into its original form by reversing the encryption.
Escrow Encryption Standard	A Federal Information Processing Standard specifying technology that provides a mechanism for the secure escrow of encryption keys, which can be used to intercept message only by government officials acting under proper legal authorization. The standard relies on a key escrow chip, known as Clipper, programmed with the classified Skipjack algorithm. Also see Clipper Chip, Capstone Chip, Skipjack, key escrow system, private key, public key cryptography.
Fiber-Optics	A method of transmitting light beams along optical fibers. A light beam, such as that produced in a laser, can be modulated to carry information. A single fiber-optic channel can carry significantly more information than most other means of information transmission. Optical fibers are thin strands of glass or other transparent material.
Frame Relay	A type of fast packet technology using variable length packets called frames. By contrast, a cell relay system, such as ATM, transports user data in fixed-sized cells.
Geosynchronous Orbit	The orbit of a satellite in which the speed and path are precisely timed to position it 22,300 miles over a fixed location on Earth.
Giga	A prefix for one billion (10^9) times a specific unit.

Gigabyte	The precise meaning often varies with the context; strictly, a gigabyte is 1 billion bytes. In reference to computers, however, bytes are often expressed in multiples of powers of two. Therefore, a gigabyte can also be either 1,000 megabytes or 1,024 megabytes, where a megabyte is considered to be 1,048,576 bytes.
Global System for Mobile Communications	A European standard for digital cellular services.
Hacker	A person who accesses or attempts to access a computer without authorization. For the purpose of this report, the term hacker refers to an external threat of unauthorized access to communications networks and related systems.
Hash Function	A technique for computing a hash total. Hash total is an error-checking value derived from the addition of a set of numbers taken from text or data. In cryptography, the recipient may use the hash function to verify a message's integrity by recalculating and verifying the hash total. If the two do not match, the original information has been changed in some way.
Hertz	A unit of frequency equal to one cycle per second.
Information Superhighway	A popular term for the emerging global broadband digital metanetwork. Also known as the national information infrastructure, infobahn, or global grid.
Interactive	Operating in a back-and-forth, often conversational manner, as when a user enters a question or command and the system immediately responds. Microcomputers are interactive machines; this interactivity is one of the features that make them approachable and easy to use.
International Data Encryption Algorithm	A block-encryption algorithm that operates on 64 bits of plaintext at a time. Developed by James Massay and Xuejia Lai at ETH, a technical institute in Zurich, the International Data Encryption Algorithm (IDEA) is perceived as a potential replacement for Data Encryption Standard. Also see Pretty Good Privacy.

Internet	Abbreviation for "internetwork." In communications, a set of computer networks—possibly dissimilar—joined together by means of gateways that handle data transfer and the conversion of messages from the sending network to the protocols used by the receiving network (with packets if necessary). When capitalized, the term "Internet" refers to the collection of networks and gateways that use the Transmission Control Protocol/Internet Protocol suite of protocols.
Interoperability	The ability of two or more systems or components to exchange information and to use the information that has been exchanged.
ISDN	Abbreviation for "Integrated Services Digital Network"—a worldwide digital communications network evolving from existing telephone services. The goal of ISDN is to replace the current analog telephone system with totally digital switching and transmission facilities capable of carrying data ranging from voice to computer transmissions, music, and video. ISDN is built on two main types of communications channels: a B channel, which carries data at a rate of 64 Kbps (kilobits per second), and a D channel, which carries control information at either 16 or 64 Kbps. Computers and other devices are connected to ISDN lines through simple, standardized interfaces. When fully implemented (possibly around the turn of the century), ISDN is expected to provide users with faster, more extensive communications services.
Japanese Digital Cellular	A Japanese standard for digital cellular services.
Key	A long stream of seemingly random bits used with cryptographic algorithms. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message.
Key Escrow System	A mechanism for the secure escrow, and controlled release, of secret or private encryption keys to law enforcement officials. Also see Escrow Encryption Standard.
Kilo	A prefix for one thousand (10^3) times a specific unit.

Last Mile	A popular term for the last segment of the connection between a communication provider and the customer. Also see local loop and on-ramps.
Local Area Network	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables a device to interact with any other on the network. Local area networks (LANS) commonly include microcomputers and shared (often expensive) resources such as laser printers and large hard disks. Most modern LANS can support a wide variety of computers and other devices. Each device must use the proper physical and data-link protocols for the particular LAN, and all devices that want to communicate with each other on the LAN must use the same upper-level communications protocol. Although single LANS are geographically limited (to a department or an office building, for example), separate LANS can be connected to form larger networks. Similar LANS are linked by bridges that act as transfer points between networks; dissimilar LANS are linked by gateways, which both transfer data and convert it according to the protocols used by the receiving network. The devices on a LAN are known as nodes, and the nodes are connected by cables through which messages are transmitted. Types of cables include twisted-pair wiring, coaxial cable, or fiber-optic (light-transmitting) cable. Nodes on a LAN can be wired together in any of three basic layouts, known as bus, ring, and star. As implied by their names, a bus network is more or less linear, a ring network forms a loop, and a star network radiates from a central hub. To avoid potential collisions when two or more nodes attempt to transmit at the same time, LANS use either contention and collision detection or token passing to regulate traffic.
Local Loop	A communication circuit connecting the telephone company central office with a subscriber's instrument. Also see last mile and on-ramps.
Mega	Abbreviated M. A prefix meaning 1 million (10^6). In computing, which is based on the binary (base-2) numbering system, mega has a literal value of 1,048,576, which is the power of 2 closest to one million.
Megabit	Abbreviated Mb or Mbit. Usually, 1,048,576 bits; sometimes interpreted as 1 million bits.

Megabyte	Abbreviated MB. Either 1 million bytes or 1,048,576 bytes.
Metanetwork	A "super" network connecting many other networks. A network of networks.
Multicast	A variant of broadcast, where information can be sent to selected recipients instead of all subscribers of a particular communications system.
Multimedia	A popular term for the integratio. . of information in a single format, for example an electronic document that may contain text, embedded voice, video, or images.
Narrowband Network	A flexible, all purpose, two-way medium that supports transmission rates under 1.5 Mbps. Also see broadband network.
National Information Infrastructure	The administration s term for the information superhighway.
Network Architecture	The underlying structure of a computer network, including hardware, functional layers, interfaces, and protocols (rules) used to establish communications and ensure the reliable transfer of information. Because a computer network is a mixture of hardware and software, network architectures are designed to provide both philosophical and physical standards for enabling computers and other devices to handle the complexities of establishing communications links and transferring information without conflict. Various network architectures exist, among them the internationally accepted seven-layer open systems interconnection model and International Business Machine (IBM) Systems Network Architecture. Both the open systems interconnection model and the Systems Network Architecture organize network functions in layers, each layer dedicated to a particular aspect of communication or transmission and each requiring protocols that define how functions are carried out. The ultimate objective of these and other network architectures is the creation of communications standards that will enable computers of many kinds to exchange information freely.

North American Dual-Mode Cellular System	A North American standard for digital cellular services.
On Ramp	A popular term for a digital broadband connection linking a subscriber with the information superhighway. Also see local loop and last mile.
Operating System	The software responsible for controlling the allocation and usage of hardware resources such as memory, the central processing unit, disk space, and peripheral devices.
Optical Fiber	A lightguide for electromagnetic waves traveling in the infrared and visible light spectrum. An optical fiber consists of two different types of glass, core and cladding, surrounded by a protective coating. The core is the light-guiding region of the fiber, while the cladding ensures that the light pulses remain within the core. One mile of fiber, capable of transmission speeds of 2,500 Mbps (2.5 gigabits per second) weighs about 1/7 of a pound. A copper cable with the same information-carrying capacity would weigh 33 tons.
Packet	In general usage, a unit of information transmitted as a whole from one device to another on a network. In packet-switching networks, a packet is defined more specifically as a transmission unit of fixed maximum size that consists of binary digits representing both data and a header containing an identification number, source and destination addresses, and, sometimes, error-control data.
Packet Switching	A message-delivery technique in which small units of information (packets) are relayed through stations in a computer network along the best route currently available between the source and the destination. A packet-switching network handles information in small units, breaking long messages into multiple packets before routing. Although each packet may travel along a different path, and the packets composing a message may arrive at different times or out of sequence, the receiving computer reassembles the original message. Packet-switching networks are considered to be fast and efficient. To manage the tasks of routing traffic and assembling/disassembling packets, such networks require some "intelligence" from the computers and software tha control delivery.

Personal Communications Network	Advanced cellular communications and the internetworking of both wire and wireless networks that are expected to offer new communications services via very small portable handsets. The network will rely on microcellular technology—many low-power, small-coverage cells—and a common channel signaling technology, to provide a wide variety of features in addition to the basic two-way telephone service.
Plaintext	Plain, unencrypted text or data.
Point of Presence	A long distance carrier's network access facility located within the service area of a local telephone company.
Pretty Good Privacy	A cryptographic software application for the protection of computer files and electronic mail. It combines the convenience of the Rivest-Shamir-Adelman public key algorithm with the speed of the secret-key IDEA algorithm, digital signature, and key management. It was developed by Philip Zimmerman, and is available globally as freeware from Internet sites or as commercial software.
Primary Rate Interface	A transmission rate interface for the integrated service digital network. It consists of 23 64 Kbps channels and one 64 Kbps channel used for signaling. Six of the 64 Kbps channels can be combined into a single 384 Kbps channel, or 24 64 Kbps channels can be combined to form a single 1.536 Mbps channel. These bundles can support applications requiring high data rates, such as video or host-to-host bulk data transfers.
Private Key	The undisclosed key in a matched key pair—private key and public key—used in public key cryptographic systems.
Private Branch Exchange	A private telephone exchange connected to the public telephone network.
Public Key	The key in a matched key pair—private key and public key—that is made public, for example, posted in a public directory, for public key cryptography.

Public Key Cryptography	Cryptography using two matched keys (or asymmetric cryptography) in which a single private key is not shared by a pair of users. Instead, each user has a key pair. Each key pair consists of a private key that is kept secret by the user and a public key that is posted in a public directory. Public key cryptography is used to perform (1) digital signature, (2) secure transmission or exchange of secret keys, and/or (3) encryption and decryption.
Real-Time System	A computer and/or a software system that reacts to events before the events become obsolete. For example, airline collision avoidance systems must process radar input, detect a possible collision, and warn air traffic controllers or pilots while they still have time to react.
Rivest-Shamir-Adelman Algorithm	A public key algorithm invented by Ronald L. Rivest, Adi Shamir, and Leonard M. Adelman. The algorithm can be used to generate digital signatures, encrypt messages, and provide key management for Data Encryption Standard and other secret key algorithms.
Secret Key	The single key that two or more parties share and keep secret for secret key cryptography. Given secret key algorithms of equal strength, the approximate difficulty of decrypting encrypted messages by brute force search can be measured by the number of possible keys. For example, a key length of 56 bits is over 65,000 times stronger or more resistant to attack than a key length of 40 bits.
Secret Key Cryptography	Cryptography based on a single key (or symmetric cryptography). It uses the same secret key for encryption and decryption.
Signaling	The process of generating and exchanging information between components of telecommunications systems to establish, monitor, or release connections (call handling functions) and to control related network and system operations and functions.
Signaling System 7	An international common channel signaling system.

Skipjack	A classified encryption algorithm. Skipjack provides high-speed encryption when implemented in a Clipper chip.
Standard	In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development. Computer standards have traditionally developed in either of two ways. The first, a highly informal process, occurs when a product or philosophy is developed by a single company and, through success and imitation, becomes so widely used that deviation from the norm causes compatibility problems or limits marketability. This type of de facto standard setting is typified by such products as Hayes modems and IBM Personal Computers. The second type of standard setting is a far more formal process in which specifications are drafted by a cooperative group or committee after an intensive study of existing methods, approaches, and technological trends and developments. The proposed standards are later ratified by consensus through an accredited organization and are adopted over time as products based on the standards become increasingly prevalent in the market.
Synchronous Operation	Generally, any operation that proceeds under control of a clock or timing mechanism.
Synchronous Optical Network (SONET)	An international standard for transmitting information over optical fiber at high speeds.
Synchronous Transmission	The serial transmission of a bit stream in which each bit occurs at a fixed time interval and the entire stream is preceded by a specific combination of bits that initiate the timing.
T-Carrier System	A hierarchy of digital transmission capabilities designed to operate at various rates, designated T1 (1.544 Mbps), T2 (6.312 Mbps), T3 (44.736 Mbps), and T4 (274.176 Mbps).
Telecommunications	A general term for the electronic transmission of information of any type, including data, television pictures, sound, facsimiles, and so on.

Telecommuting	Also called electronic commuting. The practice of working in one location (often, at home) and communicating with a main office in a different location through a personal computer equipped with a modem and communications software.
Time Division Multiple Access	A digital encoding scheme used in cellular service, this transmission method allows users to simultaneously transmit on the same frequency by allocating each user a discrete time slot.
Trojan Horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Twisted-Pair Wire	A wire made of two separately insulated strands of wire twisted together.
Virus	A computer program that can infect, replicate, and spread among computer systems. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.
Wide Area Network	A communications network that connects geographically separated areas.
Wiretapping	The real-time collection of transmitted voice or data, and the sending of that data in real time to a listening device. ("Real time" is defined as the actual time that something, such as communication of information, takes place.)
Worm	An independent computer program that reproduces by copying itself from one system to another while traveling from machine to machine across the network. Unlike computer viruses, worms do not require human involvement to propagate. Most worms and viruses are closely related—they both spread and reproduce and their effects can be identical.

Related GAO Products

Information Superhighway: Issues Affecting Development (GAO/RCED-94-285, Sept. 30, 1994).

Electronic Surveillance: Technologies Continue to Pose Challenges (GAO/T-AIMD-94-173, Aug. 11, 1994).

IRS Automation: Controlling Electronic Filing Fraud and Improper Access to Taxpayer Data (GAO/T-AIMD/GGD-94-183, July 19, 1994).

Communications Privacy: Federal Policy and Actions (GAO/OSI-94-2, Nov. 4, 1993).

IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information (GAO/AIMD-93-34, Sept. 22, 1993).

Telecommunications: Interruptions of Telephone Service (GAO/RCED-93-79FS, Mar. 5, 1993).

FBI: Advanced Communications Technologies Pose Wiretapping Challenges (GAO/IMTEC-92-68BR, July 17, 1992).

Economic Espionage: The Threat to U.S. Industry (GAO/T-OSI-92-6, Apr. 29, 1992).

Computer Security: Hackers Penetrate DOD Computer Systems (GAO/T-IMTEC-92-5, Nov. 20, 1991).

Computers and Privacy: How the Government Obtains, Verifies, Uses, and Protects Personal Data (GAO/IMTEC-90-70BR, Aug. 3, 1990).

Computer Security: Unauthorized Access to a NASA Scientific Network (GAO/IMTEC-90-2, Nov. 13, 1989).

Computer Security: Virus Highlights Need for Improved Internet Management (GAO/IMTEC-89-57, June 12, 1989).

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (301) 258-4097 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

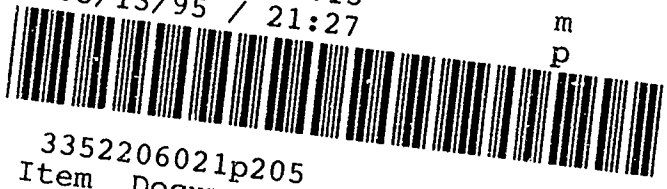
Bulk Mail
Postage & Fees Paid
GAO
Permit No. G[illegible]

Official Business
Penalty for Private Use $300

Address Correction Requested

SHIP TO:
GAIL MATHEWS
1301 PICCARD DR. S-300
ROCKVILLE MD 208504305

Request # 3352206 84 3
03/06/95 / 14:13
03/13/95 / 21:27 m
p



3352206021p205
Item Document Number
1 AIMD-95-23

BEST COPY AVAILABLE